



Internet Privacy

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

- [Background](#)
- [Electronic Communication Privacy Act](#)
- [The Children's Online Privacy Protection Act](#)
- [Anonymity](#)
- [State Laws](#)
- [Additional Resources](#)
- [Organizations](#)

Background

Among the many legal issues presented by the Internet, privacy is a leading problem. In fact, Internet privacy covers a broad range of concerns: fears about the safety of children in chat rooms and on the World Wide Web, the privacy of e-mail, the vulnerability of web users to having their Internet use habits tracked, the collection and use of personal information, the freedom of people to chat and post messages anonymously. Moreover, the rapid evolution of the Internet has frequently brought such privacy concerns before lawmakers and the courts.

Privacy concerns are frequently newsworthy. During the 1990s, child safety advocates highlighted special online dangers for children following high-profile abuse cases. Internet commerce has also been affected, too. The Federal Trade Commission (FTC) report noted in 2000 in its annual report to Congress that survey data demonstrated 92% of consumers are concerned about the misuse of personal information online. Privacy concerns over unsolicited commercial messages arose as Internet users battled to keep this so-called "spam" out of their e-mail inboxes, while in 2001, civil liberties advocates opposed potential abuse by the Federal Bureau of Investigation of its Carnivore hardware, a data-collecting technology attached to Internet services for criminal investigation.

Congress has been reluctant to enact legislation, relying upon a privacy law last revised in 1986 and passing only one new Internet privacy law in the 1990s. This was not for want of ideas. Numerous bills proposing Internet privacy protections were submitted in Congress during the late 1990s and early 2000s, and the Federal Trade Commission (FTC) also proposed legal reform. But lawmakers showed deep reservations about trifling with Internet regulation of privacy, expressing fears about hurting online commerce and creating an unenforceable regulatory scheme. Internet crime laws passed, but these criminalized intrusive and destructive behaviors without directly creating privacy rights.

The legal framework for online privacy thus rests largely on two federal laws, a subdued federal regulatory approach, a mixture of state laws, and contradictory [CASE LAW](#) from the courts:

- In 1986, Congress significantly updated the Electronic Communications Privacy Act (ECPA), originally enacted two decades earlier in 1968 to prevent telephone [WIRETAPPING](#). The law protects the privacy of much online communication, such as e-mail and other digital messaging, but far from all of it. The law offers little privacy protection to electronic communication in the workplace, which courts have further restricted.

- The Children's Online Privacy Protection Act of 1998 was passed amid complaints that websites frequently sought too much personal information from children. The law requires website operators to maintain privacy policies, grants parents powers to control information gleaned from their children by websites, and grants regulatory power to the FTC.
- Throughout the 1990s, the FTC studied and recommended proposals for new Internet privacy laws. The commission made such recommendations again in its annual 2000 report on the issue, but in 2001 new FTC leadership called for more study of the issue and a continued emphasis on self-regulation by business.
- Passed in response to the September 11, 2001 terrorist attacks upon the United States, the Patriot Act of 2001 appeared likely to significantly impact online privacy. The law dramatically increases federal police investigatory powers, including the right to intercept e-mail and track Internet usage.
- Courts have offered mixed verdicts on anonymity on the Internet. In 1997, Georgia was prohibited from enforcing a [STATUTE](#) that barred anonymous communication in *ACLU v. Miller*. In subsequent cases, courts have allowed plaintiffs to force disclosure of the identities of anonymous users of Internet message boards, but some have required that strict evidentiary standards are met by plaintiffs first.

Electronic Communication Privacy Act

Purpose of the law

The Electronic Communication Privacy (ECPA) of 1986 creates limited [STATUTORY](#) privacy rights for Internet users. First enacted in 1968, the law originally sought to prevent wiretapping by determining limits on electronic surveillance. By 1986, growing federal concern about privacy in an age of new communication technology led to a major overhaul. Lawmakers amended the ECPA to extend its privacy protection to several forms of contemporary electronic communication, from cell phones and pagers to computer transmissions and e-mail.

On the Internet the ECPA protects both digital transmissions and stored messages. In general, the law prohibits their interception or disclosure by third parties. It spells out several separate offenses:

- Intercepting or endeavoring to intercept communication
- Disclosing communication without consent
- Using electronic, mechanical, or other devices to intercept communication
- Intercepting communication for commercial purposes
- Intercepting communication for the purpose of impeding criminal investigations

Besides criminal penalties, the statute authorizes that injured parties may bring civil suits for any damages suffered, [PUNITIVE DAMAGES](#), and other relief.

Protected Internet Communication

Electronic communication is defined in broad terms as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system." Thus the ECPA extends privacy protection to everything from e-mail to drawings, pictures, and sounds as well. For communication to receive the law's protection, it cannot be simply sent between two computers: the communication must take place in the course of interstate or foreign commerce.

However, numerous exceptions are spelled out in the law. These fall into three categories:

- Limited exceptions allowing employees of network services access to communication under specific circumstances
- Broad workplace exceptions allowing employers access to employee e-mail
- Conditional government authority to carry out criminal investigations

Exceptions for Employees of Network Services

The ECPA prohibits employees of Internet providers from eavesdropping on subscribers' e-mail or other communication. However, it is not unlawful for these employees to intercept or disclose communication in the normal course of employment under two conditions:

- While engaged in the normal required performance of their jobs
- For the protection of the rights or property of the provider of the service

The statute further restricts how such exceptions may occur, specifying that "service observing" and "random monitoring" may only be carried out for mechanical or quality control checks.

Exceptions for Employers

In contrast to private home usage of the Internet, Internet communication in the workplace is given far less privacy protection under the ECPA. Underpinning this difference are philosophical assumptions about how much privacy individuals may expect at home as opposed to what they may normally expect at work. As courts have long recognized, several factors influence this question: the nature of the workplace, the relationship between employees and employers, and the legal concerns of employers are all issues that shape why the employee has a lesser expectation of privacy at work than at home.

The law permits private employers to monitor worker e-mail usage in two main ways:

- In the ordinary course of business
- When employees have given consent

Because employer monitoring of employees has been at the heart of much [LITIGATION](#), the courts have helped to define what these conditions mean. In determining whether monitoring is legal in the ordinary course of business, courts generally examine the reasons that businesses conduct the monitoring. Generally, workplace monitoring has been held to be legal under the ECPA where employers have provided notice of the policy to conduct monitoring and limited it to monitoring communication that is business-related rather than personal.

Private business and public sector employees come under different laws. While employees may give consent to monitoring, the courts have also found that "implied consent" may exist. This consent occurs when employees know or should have known that their employers intercept their electronic communications. Public sector employers are subject to a different legal standard. Monitoring in a government workplace may trigger constitutional issues such as the First Amendment right to free speech or the Fourth Amendment right to be free from an unreasonable search or seizure.

Exceptions for Government Authorities

The ECPA governs law enforcement access to private electronic communication. This statutory privacy is not absolute; however, the law recognizes that law enforcement must be able to conduct its work. But the

Encyclopedia of Everyday Law: Internet Privacy

government's power to have access to electronic communication unlimited. Like protections afforded by the Fourth Amendment to the U. S. Constitution, the law spells out limits upon government intrusion in this area of private life.

Government agents must take specific steps before intercepting communication over the Internet, gaining access to stored communication, or obtaining subscriber information such as account records and network logs from Internet service providers. Generally, they must issue subpoenas or seek and execute court orders such as search warrants. Greater degrees of invasiveness require court authority. Thus investigators can [SUBPOENA](#) basic subscriber information, but they must obtain a [SEARCH WARRANT](#) for [EXAMINATION](#) of the full content of an account.

An additional exception is created for employees or agents of the Federal Communications Commission (FCC). They may intercept or disclose communications in the normal course of employment duties or in discharging the FCC's federal monitoring responsibilities spelled out in Chapter 5 of Title 47 of the United States Code.

Additional Exceptions Under the Patriot Act of 2001

Signed into law by President George Bush on October 26, 2001, the Patriot Act of 2001 authorizes new investigatory powers for law enforcement in response to terrorist attacks upon the nation. Not all of its powers are limited to use in fighting [TERRORISM](#), however. The 350-page law amends over one dozen existing statutes, including the ECPA, for use in investigations of [COMPUTER CRIME](#) and other offenses. Some of the ECPA changes relate to the law's protections for technologies other than the Internet, but a few circumscribe the existing privacy protections for Internet communications and usage. Not all are permanent. Many are subject to sunset provisions provided by lawmakers out of concern over potential long-term harm to civil liberties.

Under the changes, law enforcement agents are able to conduct investigations with fewer legal hindrances:

- Agents may use the ECPA to compel cable Internet service providers to disclose customer Internet records without obtaining court orders.
- Agents have broader authority to obtain stored voice communications. This change to the ECPA allows agents to use a search [WARRANT](#) for examining all e-mail as well as any attachments to e-mail that might contain communication without having to seek further court authority. This change will sunset on December 31, 2005.
- Internet service providers may voluntarily make so-called "emergency disclosures" of information involving information previously prohibited from disclosure under the ECPA. This information includes all customer records and customer communications. The disclosures are permitted in situations involving immediate risk of death or serious physical injury to any person. However, the law merely permits such disclosure but does not create an obligation to make them. This change will sunset on December 31, 2005.

Without altering the ECPA, other provisions of the Patriot Act also increase police powers that potentially impact Internet privacy. These include:

- Extending the authority to trace communications on computer networks in a manner similar to tracing telephone calls, along with giving federal courts the power to compel assistance from any communication provider
- Allowing agents to obtain nationwide search warrants for e-mail without the traditional requirement that the issuing court be within the relevant [JURISDICTION](#). This change will sunset on December 31, 2005

The Children's Online Privacy Protection Act

Purpose of the law

Designed to protect minors who use the Internet, the Children's Online Privacy Protection Act (COPPA) governs how websites and online services may interact with children under 13 years of age. COPPA restricts the online collection of personal information from these young Internet users and creates certain statutory rights for their parents. Effective April 21, 2000, the law grants regulatory and enforcement authority to the Federal Trade Commission (FTC).

Who Must Comply

Businesses, groups, and individuals that collect information from children must comply with COPPA. Two broad categories exist:

- Operators of commercial websites and online services "directed to children" that collect personal information from children
- Operators of general audience websites that have actual knowledge that the site collects personal information from children

The FTC weighs several factors in determining whether a site is directed to children:

- Subject matter
- Visual or audio content
- The age of models on the site
- Language
- Whether advertising on the site is directed to children
- Information regarding the age of the actual or intended audience
- Whether a site uses animated characters or other child-oriented features

The FTC determines whether someone is a website operator by considering the following:

- Ownership and control of the information.
- Payment for the collection and maintenance of information
- Pre-existing contractual relationships
- What role the website plays in collecting or maintaining information

Basic Compliance Provisions

Under COPPA, website and online service operators must meet three main forms of compliance:

- Post their privacy policy
- Send a direct notice to parents and obtain parental consent before collecting information from children
- Obtain new consent when the site's information practices change in a material way

Privacy Policy

Operators must post a link to their privacy policy on the home page of the website or online service, as well as at each point where the site collects personal information from children. The policy must be clear and prominent and must specify the following:

Encyclopedia of Everyday Law: Internet Privacy

- Types of personal information collected, such as name, home address, email address, or hobbies
- How the site will use the information
- Whether the information is given to advertisers or third parties
- A person who may be contacted at the site

Obtaining Parental Consent

In many cases, a special notice seeking parental consent must be sent to the child's parents. The operator must notify a parent:

- That it wishes to collect personal information from the child
- That the parent's consent is required for the collection, use, and disclosure of the personal information
- How the parent can provide consent

The notice may be sent by e-mail or regular postal mail. Replies via e-mail are acceptable when the operator merely wishes to collect personal information from the child. When answers are delayed, operators may seek confirmation of consent by letter or telephone call.

Consent requirements are more strict when the operator wants to disclose a child's personal information to a third party or make the information publicly available. In such cases, the FTC requires a more reliable form of consent. Forms of consent include:

- A signed form from the parent via postal mail or fax
- Acceptance and verification of a credit card number
- Acceptance of calls from parents through a toll-free number
- E-mail accompanied by a so-called digital signature

Whenever operators make material changes to their information policies, they must send a new notice and request for consent to parents.

Exceptions Not Requiring Consent

Consent is not required when obtaining a child's e-mail address for several limited purposes:

- Responding to a one-time request from the child
- Providing notice to the parent
- Ensuring the safety of the child or the site
- Sending a newsletter of other information regularly provided parents are notified and allowed to refuse the arrangement

Parental Rights

COPPA creates two kinds of statutory rights for parents:

- Parents may compel a site to disclose both general and specific kinds of personal information they collect online from children
- Parents may revoke their consent at any time, refuse to allow further use of the child's information, and direct the operator to delete the information

Verifying Parental Identity

In order to protect children, operators must take reasonable steps to verify the parent's identity before divulging personal information:

- A signed form from the parent via postal mail or fax
- Acceptance and verification of a credit card number
- Acceptance of calls from parents through a toll-free number
- E-mail accompanied by a so-called digital signature or a PIN number or password

The law provides protection from liability under federal and state law for inadvertent disclosures of a child's information to someone who purports to be a parent.

Safe Harbors

Under COPPA, industry groups and others can create self-regulatory programs to meet compliance with the law. These so-called safe harbors require approval from the FTC.

Violations

Violations FTC rules for COPPA are treated as unfair or deceptive trade practices, punishable under the Federal Trade Commission Act.

Anonymity

The Internet has popularized the use of anonymous online identities. For privacy purposes when communicating with strangers, using public message boards, or in Internet gaming, many people avoid using their legal name and instead choose aliases. Advocates of online privacy such as the American Civil Liberties Union strongly back protections for this anonymity. Publishing anonymously has a long tradition at [COMMON LAW](#), but anonymity is not guaranteed by statute.

Legal battles over anonymity have become increasingly common since the late-1990s. In particular, companies have sought to discover the identities of their online critics by issuing subpoenas to force their disclosure. Civil liberties advocates have argued that the threat of legal action by powerful plaintiffs can stifle online speech, which, they say, depends upon anonymity. Opponents have regarded anonymity as merely cover for [DEFAMATION](#) and libel.

Courts have provided different results, and no consistent body of law exists. In an October 2000 ruling in *Hvide v. John Does*, a Florida appeals refused to overturn a lower court order that Yahoo and America Online must divulge the identities of eight anonymous message posters sought by a subpoena in a defamation lawsuit. Courts in other jurisdictions have responded differently, articulating tough evidentiary standards for obtaining subpoenas. In November 2000, a Pittsburgh state court ruled in *Melvin v. Doe* against a public official seeking to discover the identity of anonymous critic. And in *Dendrite International v. John Does*, the Superior Court of New Jersey ruled in November 2000 against a company seeking to compel disclosure of anonymous critics [ACCUSED](#) of making false statements, holding that the right of companies to sue "must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously." Case law on anonymity thus remains in flux in the early 2000s, and it is hard to predict how this area of online privacy law will develop in future years.

State Laws

Several states have enacted Internet privacy laws. Since most crime is prosecuted in state courts rather than at the federal level, states have commonly tried to keep pace with the federal government's protections. As a result, many have modeled e-mail privacy laws upon the federal Electronic Communications Privacy Act, such as New Jersey's and Pennsylvania's respective Wiretapping and Electronic Surveillance Control Acts. A number of other states protect children's privacy online, much in the way that the federal Children's Online Privacy Protection Act does. In another respect, state courts recognize common law claims involving the tort of invasion of privacy, so not all privacy rights depend upon statutory protections.

Demonstrating a strong approach to new technology issues, state legislatures have gone further than Congress in protecting e-mail privacy. Several states, such as Arkansas and Maryland, prohibit harassment through e-mail. A few address workplace concerns, with recent legislation emerging that protects employee rights. Under a Delaware law that took effect in August 2001, employers who monitor employee e-mail or Internet transmissions must inform workers about the monitoring before it begins.

Following the lead of pioneering legislation like Washington State's 1998 law, at least eighteen states have passed laws restricting how e-mail may be used by companies that send unsolicited commercial messages to consumers. Popularly known as "spam," this digital equivalent of junk mail has raised widespread concerns among private individuals who prefer not to receive it and companies that prefer not to pay the costs associated with processing it.

Anti-spam laws protect Internet service providers as well as consumers. Two of the toughest laws were passed in the late 1990s in Washington State and California. Washington State's law forbids sending commercial e-mail messages using a third party's domain name without permission, containing false or missing routing information, or with a false or misleading subject line. California's law allows Internet Service Providers to sue companies that mail spam in violation of the service's anti-spam policy, while also requiring spam to contain so-called opt-out instructions and clear labeling in the subject line describing the spam as an advertisement.

But state anti-spam laws have faced difficulties with enforcement as well as challenges to their constitutionality. Courts have reached different verdicts. In *Ferguson v. Friendfinder*, a San Francisco Superior Court judge ruled in June 2000 that key portions of California's anti-spam law were violations of the federal constitution's Commerce Clause. But in June 2001, the Washington Supreme Court upheld the constitutionality of its state anti-spam law: *State of Washington v. Jason Heckel* marked the first appeals court ruling on such cases. In October 2001, the U.S. Supreme Court declined to hear an appeal to the case, allowing the verdict to stand.

Additional Resources

"*Cyber Liberties*." American Civil Liberties Union, 2001. Available <http://www.aclu.org/issues/cyber/>

FBI Develops Eavesdropping Tools. Bridis, Ted, Associated Press, November 22, 2001.

"*Kidz Privacy*." Federal Trade Commission, 2001. Available at: <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>.

Encyclopedia of Everyday Law: Internet Privacy

Privacy Rights in a High-Tech World: Monitoring Employee E-Mail, Voicemail, and Internet Use. Morgan Lewis Counselors at Law, June 2001. Available at <http://www.morganlewis.com/wpprivacyrights.htm>.

U.S. Code, Title 13, Section 1301: Children's Online Privacy Protection Act of 1998. Available at <http://www.ftc.gov/ogc/coppa1.htm>.

U.S. Code, Title 18, Section 2510 et seq.: Electronic Communications Privacy Act of 1986. Available at <http://www.usdoj.gov/criminal/cybercrime/cclaws.html>.

You've Got Spam. Stim, Rich, [Nolo.com](http://www.nolo.com), 2001. Available at <http://www.nolo.com/encyclopedia/articles/ilaw/gotspam.html>.

West Encyclopedia of American Law. West Group, 1998.

Organizations

American Civil Liberties Union (ACLU)

125 Broad Street, 18th Floor
New York, NY 10004 USA
Phone: (212) 549-2500
URL: <http://www.aclu.org>
Primary Contact: Nadine Strossen, President

Electronic Frontier Foundation (EFF)

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

Federal Bureau of Investigation (FBI)

J. Edgar Hoover Building, 935 Pennsylvania
Avenue, NW
Washington, DC 20535-0001 USA
Phone: (202) 324-3000
URL: <http://www.fbi.gov>
Primary Contact: Robert S. Mueller III, Director

Federal Trade Commission (FTC)

CRC-240
Washington, DC 20580 USA
Phone: (877) 382-4357
URL: <http://www.ftc.gov>
Primary Contact: Timothy J. Muris, Chairman

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>