Internet Privacy

in Internet

from Gale Encyclopedia of Everyday Law

View article on Credo

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 email, 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.

Congress was initially reluctant to enact legislation, relying upon a privacy law last revised in 1986 and passing only one new Internet privacy law in the 1990s. However, Congress enacted laws in the 2000s that deal with controlling email spam and protecting children from access to Internet materials that are harmful or obscene.

Despite these new laws, the legal framework for online privacy rests largely on two federal laws, 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- In 1986, Congress significantly updated the Electronic Communications Privacy Act (ECPA), originally enacted two decades earlier in 1968 to prevent telephone **wiretapping**.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 email 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.
- Passed in response to the September 11, 2001, terrorist attacks upon the United States, the USA Patriot Act of 2001 has had a significant impact online privacy. The law dramatically increases federal police investigatory powers, including the right to intercept email and track Internet usage.

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 email.

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.

Online privacy and safety tips

Nothing online is private; the following steps help to prevent sensitive and personal information from making its rounds on the Web:

- Have more than one email account and use them for different purposes.
- Create email addresses that don't contain your full name since that can be very identifying.

Passwords

- Safest passwords contain letters, numbers and symbols. Avoid words that are in a dictionary and any important dates.
- Try not to have the same password for every account. Come up with a system that's easy to remember but will enable you to have a different password for each account.

Social networks

- Check the privacy settings and make sure it's set to the level of privacy you want. Keep in mind that even if you set your social network page to private, it doesn't guarantee that your information is completely private.
- Your friends may be able to see your other friends' posts and pages even if they're not friends with each other.
- Be aware of who's on your friend list when you post or link to certain things.
- Read the social network's privacy policy and find out who else has access to your information, such as advertisers or third-parties.

Online accounts

- Read the privacy policy. When you create an online account, whether it's to buy things, to join a group, or open an account, you should know what that site does with the information you share.
- Pay attention when creating an account. Oftentimes, this is when you can opt out of sharing personal information beyond what's necessary to create an account.
- Click “no” when it offers to check your email address book to find your “friends.” Some illegitimate sites have used this option by sending spam and viruses to everyone in your address book.
- Try not to use your name or a combination of your name as your username.

- When filling out account profiles, for increased privacy give no or very minimal information and opt out of joining the site's directory.
- For more privacy, try not to use too many applications with one account username/password. If someone guesses your username or password, they'll have access to all your applications.
- Log off when you're not using an account and do not choose to have the computer remember your passwords.

Friends and family

- Talk to your friends and family about what they can post online about you.
- Don't forget that employers, churches, sport teams, groups, and volunteer organizations that you are a part of may share your personal information online.

Safe web browsing

- Make sure you are running anti-virus and anti-spyware software and make sure that definitions are updated.
- Periodically run scans on your computer separate from your regular antivirus/antispyware.
- Periodically delete history, cookies, temporary internet files, and saved forms and passwords from your web browser.
- For added privacy, use anonymizers when you browse the web.
- Avoid searching your full legal name with information you don't want linked together

SOURCE: National Network to End Domestic Violence, Safety Net Project, 2010. Supported by US DOJ-OVW Grant #2007-TA-AX-K012. Available at http://www.nnedv.org/safetynet

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 email 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 email
- 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' email 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 email 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 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 USA Patriot Act of 2001

Signed into law by President George Bush on October 26, 2001, the USA Patriot Act of 2001 authorized 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 amended 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.

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 email as well as any attachments to email that might contain communication without having to seek further court authority.
- 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.

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 email without the traditional requirement that the issuing court be within the relevant jurisdiction.

THE CHILDREN'S INTERNET PROTECTION ACT

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program—a program that makes certain communications services and products

more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child **pornography**; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public **hearing** or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: (1) their Internet safety policies must include monitoring the online activities of minors; and (2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. In addition, the policy must bar the unauthorized disclosure, use, and dissemination of personal information regarding minors. Schools were mandated to have these policies in place by July 1, 2012.

CAN-SPAM ACT

The onslaught of “spam” commercial email became a concern within a few years of the Internet's growth in popularity. Users complain about the invasion of their privacy by unwanted email messages. Congress responded by enacting the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003. The act covers all commercial messages, which the law defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,” including email that promotes content on commercial websites. The law makes no exception for business-to-business email. Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.

Federal rules require that commercial email messages must clearly identify themselves as a **solicitation** or advertisement for products or services. In addition, the email must provide an “opt-out” provision: an easily-accessible, legitimate, and free way for the receiver of the message to reject future messages from that sender. Finally, the email must contain legitimate return email addresses, as well as the sender's postal address. These provisions apply to mobile phones and commercial text messages as well as traditional computer email.

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. However, it has become more common for plaintiffs in

defamation and libel cases to obtain the name of the Internet poster.

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 email privacy laws upon the federal Electronic Communications Privacy Act, such as New Jersey's and Pennsylvania's respective Wiretapping and Electronic Surveillance Control Acts. 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 email privacy. Several states, such as Arkansas and Maryland, prohibit harassment through email. A few address workplace concerns, with recent legislation emerging that protects employee rights. Under a Delaware law, employers who monitor employee email or Internet transmissions must inform workers about the monitoring before it begins.

Following the lead of pioneering legislation like Washington State's 1998 law, 37 states have passed laws restricting “spam” email messages. Most of these laws prohibit misrepresenting or falsifying the origin of or the routing information on messages; using an Internet address of a third party without permission, or including misleading information in the subject line of a message. Some states also prohibit the sale or distribution of software that is designed solely to falsify or forge the point of origin of or the routing information on email messages. Most other parts of state laws, such as labeling requirements for adult-oriented advertising, are pre-empted by the federal CAN-SPAM Act. This law pre-empts any state law that “expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.”

ADDITIONAL RESOURCES

- Gale Encyclopedia of American Law. 3rd ed. Gale, Cengage Learning Detroit, 2011.
- Lessig, Lawrence. Code: And Other Laws of Cyberspace, Version 2.0. Basic Books New York, 2006.
- Rustad, Michael L. Internet Law in a Nutshell. West, Thomson Reuters Eagan MN, 2009.
- Weaver, Russell. From Gutenberg to the Internet: Free Speech, Advancing Technology, and the Implications for Democracy. Carolina Academic Press Durham NC, 2012.

ORGANIZATIONS

- American Civil Liberties Union (ACLU) 125 Broad St., 18th Fl. New York NY 10004 Phone: (212) 549-2500 Email: info@aclu.org URL: http://www.aclu.org/.
- Electronic Frontier Foundation (EFF) 454 Shotwell Street San Francisco CA 94110 Phone: (415) 436-9333 Fax: (415) 436-9993 URL: http://www.eff.org.
- Federal Bureau of Investigation J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW Washington, DC 20535-0001 Phone: (202) 324-3000 URL: http://www.fbi.gov.
- Federal Trade Commission (FTC) CRC-240 Washington, DC 20580 Toll Free: (877) 382-4357

URL: http://www.fbi.gov.

APA

Internet privacy. (2013). In Gale (Ed.), *Gale encyclopedia of everyday law* (3rd ed.). Gale. Credo Reference: https://search.credoreference.com/content/entry/galegel/internet_privacy/0

Chicago

"Internet Privacy." In *Gale Encyclopedia of Everyday Law*, edited by Gale. 3rd ed. Gale, 2013. https://search.credoreference.com/content/entry/galegel/internet_privacy/0

Harvard

Internet privacy. (2013). In Gale (Ed.), *Gale encyclopedia of everyday law*. (3rd ed.). [Online]. Farmington: Gale. Available from: https://search.credoreference.com/content/entry/galegel/internet_privacy/0 [Accessed 22 November 2021].

MLA

"Internet Privacy." *Gale Encyclopedia of Everyday Law*, edited by Gale, 3rd edition, 2013. *Credo Reference*, https://search.credoreference.com/content/entry/galegel/internet_privacy/0. Accessed 22 Nov. 2021.