Privacy Organizations and Initiatives

By Gary Bahadur, William Chan, Chris Weber

Apr 12, 2002

Sample Chapter is provided courtesy of Que

Find out how some organizations are fighting to protect your right to privacy, even as technology becomes steadily more invasive. Guidelines for privacy are still not defined or protected. For consumers to feel secure in using the Internet and other technologies while protecting who they are from prying eyes, corporations and governments must find a mixture of government and corporate compromise that will ensure we remain anonymous in an ever more connected world.

This chapter is from the book
Privacy Defended: Protecting Yourself Online

The consumer on his own stands no chance of defending his own privacy needs. The lack of power by the individual consumer has given rise to a number of organizations that should lessen the burden of fighting the "forces of evil" that would take away all our privacy rights. "Forces of evil" might be a strong term, but how else to describe companies and governments that would strip others of an inherent right to be left alone and to keep our personal information confidential?

The U.S. government has failed to set the standards and controls necessary to ensure our privacy. It has been the task of the privacy industry, organizations, and individuals to create these standards. The government has even failed to meet its responsibilities on the standards of privacy. In 2000, the government banned cookies from most government sites, yet reports of 51 inspectors general found 300 cookies on the Web sites of 23 agencies that should not have been there. *Cookies*, as we mentioned in earlier chapters, track user information and browsing preferences. "These reports document a real problem—the violation of Americans' privacy by their own government on the Internet," said Sen. Jay Inslee, (D-Wash). Auditors from that agency learned three contractors who maintained Web sites for government departments were collecting personal information, such as Social Security numbers, without disclosing how they used that information.

The findings also showed that Web *bugs* were found on 23 Commerce Department pages (these bugs collect information), and nearly 75% of State Department sites were not in compliance with government rules requiring agencies to post their privacy policies. Several contractors who maintain government sites were collecting personal information such as Social Security numbers without notifying users how this information would be used. Other government agencies, such as the Federal Trade Commission, are also not becoming involved in privacy issues. FTC Commissioner Thomas Leary said, "We're a lot more relaxed than we were before." It's hard to imagine the government being any more relaxed about our privacy rights. Leary also said, "This hysteria [over privacy] is misplaced." If the government can't even comply with it own privacy standards and has such little regard for our privacy, how will the consumer achieve any level of personal information security?

Although many think government involvement in privacy issues is desirable, some feel less government involvement and more private industry controls are the right way to achieve consumer privacy needs. According to a report released in May 2001 by Citizens Against Government Waste (CAGW), it would be cheaper on Americans for private industry to regulate itself rather than having Congress pass laws and trying to enforce those laws. CAGW's new study, "Keeping Big Brother From Watching You," concluded that "federal privacy regulations or legislation are unnecessary and that the private sector is

more effective than government in this increasingly important area." The 107th session of Congress has put forth more than 40 bills aimed at privacy; whether all these pass or actually benefit the consumer has been highly debated. If the government can't handle the laws that have already been passed, how will new laws be enforced to protect the consumer? Organizations such as CAGW promote private sector policies to help consumers and want the government to continue with its hands-off approach to privacy.

Another study released in May 2001, underwritten by the Association for Competitive Technology (ACT), a Microsoft-backed lobbying organization, found that privacy laws could cost businesses between $9 billion and $36 billion. Firms were asked to estimate their charges to make the changes required under several pending bills to determine what the potential costs to the industry would be. The costs range anywhere from $100,000 on up to the millions. Fourteen of the 17 companies questioned are affiliated with ACT. This is not an impartial study, but it does shed some light on potential costs of privacy laws. Groups such as ACT also want a government hands-off approach but for different reasons from organization such as CAGW. With less government involvement, private industry can more easily turn a profit in just about anything it does.

Privacy Organizations

A lack of government intervention in protecting consumer privacy rights has caused grassroots efforts to spring up to address the void in privacy organizations. Publicly funded nonprofit organizations have taken on the challenge of fighting for consumer privacy rights. The following sections discuss several of the key players when it comes to organizations taking on the battle against business and government threats to your privacy.

Online Privacy Alliance

http://www.privacyalliance.org

The Online Privacy Alliance (OPA) is a group of corporations and associations that attempts to promote online privacy initiatives. The OPA is in favor of self-regulation of privacy concerns and less government involvement. The mission of the alliance is stated as follows:

"The Alliance will:

- identify and advance effective online privacy policies across the private sector
- support and foster the development and use of self-regulatory enforcement mechanisms and activities, as well as user empowerment technology tools, designed to protect individuals' privacy
- support compliance with and strong enforcement of applicable laws and regulations
- support and foster the development and use of practices and policies that protect the privacy of children
- promote broad awareness of and participation in Alliance initiatives by businesses, non-profits, policy makers, and consumers
- seek input and support for Alliance initiatives from consumer, business, academic, advocacy and other organizations that share its commitment to privacy protection."

Several of its larger members include IBM, Microsoft, Verizon, The American Institute of Certified Public Accounts, and Sun Microsystems. The OPA reports on privacy news and provides resources for companies and consumers to learn more about privacy issues. The OPA has set up guidelines for defining a privacy policy that companies can use and a framework for enforcing self-regulation. The guidelines have become an industry framework for the creation of a privacy policy.

OPA has been active in lobbying government officials to promote self-regulation. One such action was focused on the Congressional Privacy Caucus. The Privacy Caucus includes more than 30 members of Congress from the House and Senate. It is co-chaired by Sens. Richard Shelby (R-AL) and Chris Dodd (D-CT) and Reps. Joe Barton (R-TX) and Edward Markey (D-MA). The OPA wants laws to focus on privacy issues and not the technologies being used. "It's the behavior of businesses and not the technologies they use that determine whether consumer privacy is respected," said Christine Varney, an advisor to the OPA. Another initiative by the OPA was the submission of comments to the Department of Health and Human Services (HHS) regarding their proposed implementation of the provisions of the Health Insurance Portability and Accountability Act of 1996. The regulations are unclear, and the implementation of controls to comply with the regulations is not defined. The OPA attempts to empower and educate consumers on how to protect their privacy online.

BBBOnline

http://www.bbbonline.org

BBBOnline is a subsidiary of the Council of Better Business Bureaus. Its mission is to "promote trust and confidence on the Internet through the BBBOnline Reliability and BBBOnline Privacy programs." BBBOnline has three certification programs called the Reliability Seal Program, Kids Privacy Seal Program, and Privacy Seal Program. A Web site can get these seals to show that they promote privacy initiatives and give consumers some form of confidence that the site is trustworthy. This is a self-regulatory program for Web sites. Several of the criteria for a Web site getting the Seal include

- Being members of their local Better Business Bureaus
- Having been in business for at least one year
- Having agreed to abide by BBB standards of truth in advertising
- Having committed to work with the BBB to resolve consumer disputes that arise over goods or services promoted or advertised on their site
- Providing the BBB with information regarding company ownership and management and the street address and telephone number at which they do business
- Agreeing to participate in the BBB's advertising self-regulation program
- Responding promptly to all consumer complaints

After it's approved, a company is allowed to put on its Web site the seals shown in Figures 3.1, 3.2, and 3.3.

Figure 3.1 BBBOnline Reliability seal.

Figure 3.2 BBBOnline Kids Privacy seal.

Figure 3.3 BBBOnline Privacy seal.

The Kids Privacy Seal Program is used by a Web site to show that it is in compliance with the Children's Online Privacy Protection Act (COPPA). This law requires all businesses with any part of their Web sites (or online services) directed at children under the age of 13 or Web sites (or online services) that collect personally identifiable information from visitors actually known to be under the age of 13 to follow specific guidelines. These requirements to get this seal are based on the guidelines of the Council of Better Business Bureaus' Children's Advertising Review Unit (CARU), the industry standards suggested by the Online Privacy Alliance, and the Children's Online Privacy Protection Act.

Several of the criteria required to get this seal include

- The Web site must obtain parental consent before any personally identifiable information can be collected, used, or disclosed.
- The Web site must obtain parental consent before children are allowed to post or communicate directly with others.
- The Web site must provide warnings and explanations in easy-to-understand language.
- The Web site must avoid collecting more information than necessary when offering children's games and activities.
- The Web site must be careful in the way it provides hyperlinks.
- The Web site must follow strict rules when sending e-mail.
- The Web site must provide reasonable access to collected information.

BBBOnline is more of a resource for information than an enforcer of privacy initiatives. A company can tout that it has the seal, but no concrete measures or procedures define how a consumer's informationis handled. The seals do not say that the company will not resell your information or use cookies on its site to track your information. BBBOnline has little authority to do anything about a compromise of your information after a company has the seal. As we captured the image of the seal for this book, what is to stop a Web site from copying the image and putting it on it sites even if it is not a BBBOnline member?

It might even be said that these seals are counterproductive. If a consumer goes to a site with this seal, she might have a false sense of security, which is worse than knowing your data is insecure. If you think this seal will protect your private information and then submit personal data to a site, you do not really know how the company will treat your information if you did not read its privacy policy. If, at the time the company got the seal, it had great privacy measures in place, there is no guarantee that a week later its policies did not change. If it changed its policies after getting the seal, what is the follow-up mechanism for notifying consumers and notifying BBBOnline of the changes? The lack of defined procedures for

ensuring the seal actually provides some value to the consumer makes these type of programs of limited value to the consumer. Several other such programs can also be misleading to the consumer, as we will discuss later.

TRUSTe

http://www.truste.org

TRUSTe is an endeavor similar to BBBOnline. Its goal is to promote Internet privacy and provide a seal of approval to sites that meet its requirements. It has a number of sponsors and contributor companies that help promote the seals. Like BBBOnline, it is also an information repository for privacy initiatives. To be approved for the Privacy Seal (see Figure 3.4), the Web site seeking approval must meet the following criteria:

- Adoption and implementation of a privacy policy that takes into account consumer anxiety over sharing personal information online
- Notice and disclosure of information collection and use practices
- Choice and consent, giving users the opportunity to exercise control over their information
- Data security and quality and access measures to help protect the security and accuracy of personally identifiable information

Figure 3.4 The TRUSTe Privacy seal.

The TRUSTe seal informs the consumer that the site will disclose the following:

- What personal information is being gathered about you
- How the information will be used
- Who the information will be shared with, if anyone
- Choices available to you regarding how collected information is used
- Safeguards in place to protect your information from loss, misuse, or alteration
- How you can update or correct inaccuracies in your information

Similar to BBBOnline, TRUSTe also has a Children's Privacy Seal, as shown in Figure 3.5. This applies to children under the age of 13. TRUSTe has also recently been approved as a "safe harbor" program under the terms of the Children's Online Privacy Protection Act. Safe harbor programs are industry self-regulatory guidelines that are deemed to implement the act. The Children's Privacy Seal notifies the consumer that the site will not

- Collect online contact information from a child under 13 without prior verifiable parental consent or direct parental notification of the nature and intended use of this information, which shall include an opportunity for the parent to prevent use of the information and participation in the activity. Where prior parental consent is not obtained, online contact information shall only be used to directly respond to the child's request and shall not be used to recontact the child for other purposes.
- Collect personally identifiable offline contact information from children under 13 without prior verifiable parental consent.
- Distribute to third parties any personally identifiable information collected from a child under 13 without prior verifiable parental consent.
- Give the ability to children under 13 to publicly post or otherwise distribute personally identifiable contact information without prior verifiable parental consent, and will make best efforts to prohibit a child from posting any contact information.
- Entice a child under 13 by the prospect of a special game, prize, or other activity to divulge more information than is needed to participate in such activity.

Figure 3.5 TRUSTe Kids Privacy seal.

Several differences exist between TRUSTe and BBBOnline. Although they both have a dispute resolution service for when a member carrying the seal does not comply with the requirements, the seal by TRUSTe has more details and a check mechanism to ensure that the site displaying a seal is actually a member of the program (see Figure 3.6). The mechanism to check whether a site is actually part of the TRUSTe program is very proactive and takes a step in the right direction. The only problem with this is that a consumer must click the icon to check the site. Most consumers do not check each site they visit to determine whether the site is actually a member of the TRUSTe Program.

Figure 3.6 TRUSTe Click-to-Verify seal.

As with the BBBOnline seal, after a company is approved for this seal, it's hard to continue to verify that its polices and practices haven't changed and therefore break the requirements of the seal. TRUSTe does make the attempt to keep sites in compliance, but there will be a window between the change and checkup by TRUSTe when a site could be compromising consumer privacy. TRUSTe's policy on checkup on compliance with its criteria is as follows:

- Initial and periodic reviews of the site by TRUSTe
- "Seeding," whereby the company submits personal user information online to verify that a site is following its stated privacy policies
- Compliance reviews by a CPA firm
- Feedback and complaints from the online community

Electronic Information Privacy Organization

http://www.epic.org

The Electronic Information Privacy Organization (EPIC) is a nonprofit organization dedicated to serving the public's civil liberties and privacy. EPIC is involved with other privacy organizations such as Privacy International (http://www.privacyinternational.org), the Global Internet Liberty Campaign (http://www.gilc.org), the Internet Free Expression Alliance (http://www.ifea.net), the Internet Privacy Coalition (http://www.crypto.org), the Internet Democracy Project (http://www.internetdemocracyproject.org), and the Trans Atlantic Consumer Dialogue (http://www.tacd.org). EPIC is actively pursuing government legislation and fighting laws that would compromise consumer privacy. The Web site provides a wealth of privacy information and keeps up-to-date with the latest laws being passed and that are being proposed. EPIC is funded by consumer and corporations who want to promote the fight for privacy.

Recently, EPIC's executive director, Marc Rotenberg, testified before the House Commerce Committee on Information Privacy urging Congress to pass privacy legislation and promote technology that would better secure consumer information. EPIC often brings privacy matters to the forefront of congressional business to protect consumers. One such matter brought to Congress's attention was the proposed sale of consumer domain name registration information by Network Solutions to direct marketing companies. The following is an excerpt from the letter sent to Congress by EPIC:

Electronic Privacy Information Center

February 16, 2001

Representative Fred Upton
2333 Rayburn House Office Building
Washington, DC 20515

Representative Edward J. Markey
2108 Rayburn House Office Building
Washington, DC 20515

Senator Conrad Burns
187 Dirksen Senate Office Building
Washington, DC 20510

Senator Fritz Hollings
125 Russell Senate Office Building
Washington, DC 20510

Dear Congressmen,

We are writing to you on behalf of the Electronic Privacy Information Center (EPIC) to bring your attention to a privacy issue of importance to Internet users around the world, and of particular concern to users in the United States who register domain names. According to a report in *The Wall Street Journal* today, Network Solutions, Inc., the largest domain registration company in the country, is now selling information on 6 million Internet customers to direct marketers. The information was obtained by Network Solutions, Inc. for the purpose of registration and is not unlike motor vehicle information for which Congress has passed important privacy legislation, The Drivers Privacy Protection Act of 1994, that was recently upheld by the United States Supreme Court in Reno v. Condon, 528 U.S. 141.

We are writing to you to urge you to examine whether this sale is currently permissible and if so, whether it is therefore necessary to adopt new legislation to safeguard the information that is provided by Internet users and companies as a condition of registering a domain name. We believe that the sale violates well established principles of U.S. law as well as international privacy standards, including privacy rules specifically developed to address concerns related to privacy in the context of domain name registration.

Thus far privacy has received only passing attention during the discussion of ICANN's authority. The Subcommittee on Communications recently held hearings on the Internet Corporation for Assigned Names and Numbers, otherwise known as ICANN. ICANN is the central authority for all Internet users

worldwide that wish to register a domain name. As mentioned during the recent hearings held by your Subcommittee, part of ICANN's responsibility is to protect the privacy of its domain name registrants. Also mentioned during the hearings was the low level of privacy protection offered for this personal information. As you pursue further work on ICANN, we urge you to focus on the much-needed privacy protections for this personal information.

Another case of EPIC's fight for consumer privacy was when it filed a letter of complaint against the company eTour. The letter sent to the Federal Trade Commission (FTC) and the National Association of Attorneys General (NAAG) alleged that direct-marketing company eTour, Inc., violated consumer protection law by selling personal information about its 4.5 million customers to Ask Jeeves in early 2001, despite clear statements that it would never do so. eTour's privacy policy was vague on what constitutes a breach of its privacy policy.

EPIC also testified on Social Security number privacy in May of 2001 before the U.S. House of Representatives Subcommittee on Social Security. A hearing was held on "Protecting Privacy and Preventing Misuse of Social Security Numbers." EPIC argued the point that "legislation to limit the collection and use of the SSN is appropriate, necessary, and fully consistent with U.S. law."

Unlike ACT, EPIC seeks to have more government intervention, or at a minimum, the government intervention that actually promotes consumer privacy. EPIC launched an Internet Public Interest Opportunities Program (IPIOP) that will serve law students who have an interest in public interest law and the Internet. EPIC uses the Freedom of Information Act (FOIA) to obtain information from the government about cryptography and privacy policy. Several cases that EPIC has been involved with include the following:

- **Electronic Privacy Information Center v. Department of Justice & Federal Bureau of Investigation (C.A. No. 00-1849)**—EPIC wanted to make details of DCS1000 public.
- **Electronic Privacy Information Center v. National Security Agency (C.A. No. 99-3197)**—EPIC asked a federal court to order the release of controversial documents concerning government surveillance of American citizens and sought public disclosure of internal National Security Agency (NSA) documents.
- **Electronic Privacy Information Center v. Federal Trade Commission (C.A. No. 99-2689)**—Sought the disclosure of records about privacy complaints received by the Federal Trade Commission.
- **Electronic Privacy Information Center v. U.S. Department of State (C.A. No. 97-1401)**—Sought public disclosure of the travel records of Ambassador David Aaron, who has been promoting the Administration's controversial encryption policies in foreign countries. EPIC is seeking to open U.S. encryption policy to public scrutiny.
- **Electronic Privacy Information Center v. U.S. Department of State (C.A. No. 95-2228)**—Sought the release of a survey conducted by the Department of Commerce (DOC) on the foreign availability of encryption software.
- **Electronic Privacy Information Center v. National Security Council (C.A. No. 95-0461)**—Sought disclosure of information concerning the Security Policy Board.

Several of the laws discussed in Chapter 2, "Defining Privacy: Social and Legal Aspects," can either help or hurt consumer privacy rights. EPIC advocates laws that enforce privacy initiatives and protect the consumer. Fighting companies that take advantage of users is also one of EPIC main concerns as demonstrated by the fight against eTour and Network Solutions.

Federal Trade Commission

http://www.ftc.gov

The Federal Trade Commission (FTC) is one of the few government organizations that has been actively involved with privacy concerns of consumers. The Internet has led to an enlargement of the scope of the FTC's activities. No longer are they just concerned with communications mediums such as telephone, radio, and TV. The Internet has posed new challenges for the power and enforcement capabilities of the FTC. One of the main functions of the FTC Web site is to educate consumers about laws and privacy initiatives.

The FTC has launched various initiatives to safeguard consumer privacy. Some of the focus revolves around credit bureaus, the Department of Motor Vehicles (DMV), and Direct Marketers.

The three major credit bureaus the FTC has focused on helping consumers protect that privacy include

- Equifax, Inc., P.O. Box 740123, Atlanta, GA 30374-0123
- Experian, 701 Experian Parkway, Allen, TX 75013
- Trans Union, P.O. Box 97328, Jackson, MS 39288-7328

Each of these agencies has opt-out options the FTC wants consumers to know about.

Similar to credit bureaus, the DMV has a lot of personal information about you. Even though the Drivers Protection Act has some safeguards against distributing your personal information, the DMV still has a lot of leeway in disseminating information. Information can be given to law enforcement, driver safety agencies, background checking agencies, insurance brokers, and a host of other agencies. However, few people can get your DMV information. The FTC does make an effort to educate consumers of the possibilities of how your information can be used through DMV.

As we have plainly seen, direct marketing can be very intrusive, and direct marketers can easily find out a lot of information about your preferences. The Direct Marketing Association (http://www.the-dma.org) offers the Mail, Telephone, and E-mail Preference Services, which allow you to opt out of some marketing databases. The FTC publishes a free brochure on "Shopping by Phone or Mail" to assist consumers is taking some steps to protect themselves.

The FTC is also involved in policing efforts for numerous laws. One that concerns consumer privacy is the Gramm-Leach-Bliley Act. As mentioned in Chapter 2, the act removes certain restrictions on mergers, affiliations, and other business activities of banks that date to the Depression era. The concerns about privacy cause amendments to the act that try to protect consumer privacy and sharing of information between entities. The FTC is one of the agencies responsible for ensuring compliance with the act. Another major act the FTC has responsibility in policing is the HIPAA Act. HIPAA and Gramm-Leach-Bliley address similar regulatory concerns and contain several common compliance elements the FTC must address and ensure that companies are in compliance with. As with most government agencies' involvement with private industry, there is much confusion and no clear decision on compliance and how the FTC will address the necessary steps to ensure compliance.

The FTC has also been aggressively pursuing privacy violations. In one recent case, the FTC successfully prosecuted three Web sites that were in violation of the Children's Online Privacy Protection Rule (COPPA Rule). The FTC charged Monarch Services, Inc., and Girls Life, Inc., operators of http://www.girlslife.com Bigmailbox.com, Inc., and Nolan Quan, operators of http://www.bigmailbox.com and Looksmart Ltd., operator of http://www.insidetheweb.com, with illegally collecting personally identifying information from children under 13; these companies settled with the FTC on these charges. The FTC has also settled a case with Toysmate.com, which violated its privacy policy that stated it would never sell consumer information. The FTC also settled a case against several online pharmacies, including Worldwidemedicine.com and Focusmedical.com, which misrepresented information to consumers and did not handle consumer information securely. COPPA has helped increase the number of sites posting a privacy policy from 24% in 1998 to 91% today. The FTC also grants "safe harbor" status to companies and associations that prove they are in compliance with COPPA. The Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus—an arm of the advertising industry's self-regulatory program—won the first COPPA safe harbor approval, which the FTC is striving for many companies to achieve.

Government agencies such as the FTC that strive to assist companies with securing consumer privacy rights are themselves subject to privacy violations. In July 2001, the U.S. Department of Commerce's safe harbor Web site was hacked by attackers. Safe harbor participants were contacted about the attack. The lack of security on government sites can greatly discourage companies that are seeking guidance from government agencies regarding the steps they must take to protect their consumers.

Privacy International

http://www.privacyinternational.org

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. It is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy. This information portal does not have any authority or government powers and serves only as a consumer education site.

Several initiatives that PI has recently conducted include the following:

- **International Privacy Survey**—Reviews the state of privacy in more than 50 countries of privacy issues including, data protection, telephone tapping, genetic databases, ID systems, and freedom of information laws.
- **Project Compliance**—Monitors companies' compliance with the EU Data Protection and the U.S./EU negotiations on Safe Harbor.
- **Big Brother Awards**—"Awards" are given to the companies, government agencies, and individuals that have most directly undercut privacy.

Privacy.org

http://www.privacy.org/

Privacy.org is the site for daily news, information, and initiatives on privacy, striving to educate consumers about the actions of companies and governments to compromise their privacy. The Web site is a joint project of EPIC and Privacy International. On this site are a number of links and resources to further information to protect consumer privacy.

Internet Free Expression Alliance

http://www.ifea.net

The Internet Free Expression Alliance (IFEA) is another informational site that seeks to educate consumers on privacy issues with an emphasis on freedom of expression. The IFEA seeks to protect the privacy of such entities as Internet users, online publishers, libraries, and academic groups. A number of organizations belong to the IFEA to promote free speech issues.

From the IFEA Web site, the goals of the Internet Free Expression Alliance include

- Ensure the continuation of the Internet as a forum for open, diverse, and unimpeded expression and to maintain the vital role the Internet plays in providing an efficient and democratic means of distributing information around the world
- Promote openness and encourage informed public debate and discussion of proposals to rate and/or filter online content
- Identify new threats to free expression and First Amendment values on the Internet, whether legal or technological
- Oppose any governmental effort to promote, coerce, or mandate the rating or filtering of online content
- Protect the free speech and expression rights of both the speaker and the audience in the interactive online environment
- Ensure that Internet speakers are able to reach the broadest possible interested audience and that Internet listeners are able to access all material of interest to them
- Closely examine technical proposals to create filtering architectures and oppose approaches that conceal the filtering criteria employed, or irreparably damage the unique character of the Internet
- Encourage approaches that highlight "recommended" Internet content, rather than those that restrict access to materials labeled as "harmful" or otherwise objectionable, and emphasize that any rating that exists solely to enable specific content to be blocked from view can inhibit the flow of free expression

Electronic Frontier Foundation

http://www.eff.org

The Electronic Frontier Foundation (EFF) is a nonprofit, nonpartisan organization that is member supported. The organization seeks to protect civil liberties, including privacy and freedom of expression on the Internet. EFF was founded in 1990 and is based in San Francisco, California. Like other sites such as PI and IFEA, the EFF is a strong advocate for consumer freedom. The EFF speaks to law enforcement organizations, state attorney bar associations, conferences and summits, and university classes and takes an active role in pursuing legal action and helping victims of privacy invasion and freedom of speech restrictions. The EFF has taken active roles in many cases, including the following:

- **Felten v. RIAA**—EFF asked a federal court to rule that Princeton University professor Edward Felten and his research team have a First Amendment right to present their research on digital music access-control technologies at the USENIX Security Conference this August in Washington, D.C.
- **DVD-CCA v. Bunner**—The DVD Copy Control Association (DVD-CCA) is suing dozens of individuals who put DeCSS (a program to decrypt the protections placed on DVDs) on their Web sites. The EFF is paying for and coordinating the case.
- **Medinex_v._Awe2bad4mdnx**—The EFF is defending critics of a failing dot.com company to defend the right of anonymous critics to express their views online without fear of arbitrary disclosure of their identities. The company called Medinex Systems, Inc., seeks to learn the identities of 14 John Does who participated in a Yahoo! message board. On May 21, 2001, Medinex dismissed the suit before a hearing could be held. EFF provided pro bono defense for the anonymous posters.

EFF submits amicus briefs and finds pro bono counsel when possible for other free-speech cases. EFF has been very active in protecting the Children's Internet Protection Act. The EFF is also against implementation of Congressionally mandated Internet blocking in schools and libraries as outlined in this act and works with other privacy groups to protect such laws. Lisa Maldonado, field director for the American Civil Liberties Union of Northern California commented, "The government is trying to strangle the free flow of information on the Internet to those library patrons who need it the most. CHIPA would widen the 'digital divide' that already exists between those who can afford Internet access at home and those who rely on their public library for Internet access." "The government-mandated requirement for Internet blocking in schools and libraries violates the free expression rights of Americans, adults and minors alike," said Will Doherty, EFF online activist.

Global Internet Liberty Campaign

http://www.gilc.org

Another education and information dissemination organization, the Global Internet Liberty Campaign (GILC), was formed by members of the American Civil Liberties Union, the Electronic Privacy Information Center, Human Rights Watch, the Internet Society, Privacy International, the Association des Utilisateurs d'Internet, and other civil liberties and human rights organizations. GILC members speak out against laws and initiatives that can infringe on consumer privacy. Several statements released by the GILC include opposition to stealth blocking, which is the practice of some Internet service providers (ISPs) to block Internet access to particular hosts without the knowledge of end users and opposing the DVD Copy Control Association's (CCA) suit against people who have posted information about the DVD Content Scrambling System (CSS).

From the Organization's Web site, the GILC advocates the following:

- Prohibiting prior censorship of online communication
- Requiring that laws restricting the content of online speech distinguish between the liability of content providers and the liability of data carriers
- Insisting that online free expression not be restricted by indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components of the Internet
- Including citizens in the Global Information Infrastructure (GII) development process from countries that are currently unstable economically, have insufficient infrastructure, or lack sophisticated technology
- Prohibiting discrimination on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status
- Ensuring that personal information generated on the GII for one purpose is not used for an unrelated purpose or disclosed without the person's informed consent and enabling individuals to review personal information on the Internet and to correct inaccurate information
- Enabling online users to encrypt their communications and information without restriction

Junkbusters

http://www.junkbusters.com

This site provides a great deal of information about removing yourself from mass mailing and e-mailing lists. The site mission is "to get rid of any junk mail, telemarketing calls, junk faxes, junk pages, junk e-mail, unwanted banner ads, and any other solicitations" you do not want. As we have seen so far, this is a major undertaking. The site provides educational information on such things as cookies, Web bugs, and how to reply to marketers to get your name off mailing lists.

Share This Your Account **Page 1** of 3 Next >

Discussions

Make a New Comment

You must log in in order to post a comment.