

Facts About

Privacy and Cyberspace



*“Facts are stubborn things;
and whatever may be our wishes,
our inclinations, or the dictates
of our passions, they cannot
alter the state of facts
and evidence.”*

— John Adams, December 1770



American Bar Association

Division for Media Relations and Communication Services

Acknowledgments

Special thanks to ABA Publishing, *Human Rights* magazine, and the ABA Section of Business Law for providing many of the source materials used in developing *Facts About Privacy and Cyberspace*. We are grateful to Sarina Butler, Amelia Boss, Richard Greenstone, Jane Kirtley, Charles Mudd, Ray Ocampo, Thomas Smedinghoff, and George Trubow for their invaluable comments and suggestions. *Facts About Privacy and Cyberspace* was prepared by Paul Marcotte of the American Bar Association Division for Media Relations and Communication Services and designed by Gail Patejunas. Additional information and assistance was provided by Angie Burke, Al Manning and Deborah Weixl of the Media Relations staff.

You may republish or cite any portion of this work, with the following attribution:
“Reprinted by permission from *Facts About Privacy and Cyberspace*. Copyright © 2000 American Bar Association. All rights reserved.”

Table of Contents

Introduction		Page
Sources of Information		
Question 1	What information is collected by government agencies?	1
Question 2	Is the information public?	1
Question 3	Are public records available online?	1
Question 4	What other information about people is available online?	2
The Importance of Privacy		
Question 5	What can happen if someone’s privacy isn’t protected?	3
Question 6	Why is this a particular problem in cyberspace?	3
Protecting Privacy		
Question 7	Are there any laws governing dissemination of information collected by government entities and others?	5
Question 8	How much privacy can someone expect when they are online?	5
Question 9	What are some clearly public activities?	6
Question 10	Can online services and web sites access information stored on someone’s computer without their knowledge?	6
Question 11	How can people protect their privacy in cyberspace?	7
Question 12	What is encryption?	7
Question 13	How effective is encryption in ensuring privacy?	8
Children on the Internet		
Question 14	How do web sites gather information about children?	9
Question 15	Are there any laws regulating this?	9
Question 16	Can web sites get around the law by gathering information about children from cookies?	10

Question 17	What special risks do Internet chat rooms pose for children?	10
Question 18	How can parents protect their children online?	11

E-Mail Privacy in the Workplace

Question 19	Is there federal law covering e-mail privacy in the workplace?	12
Question 20	Do state laws offer any protections to e-mail?	12
Question 21	What about common law privacy?	13
Question 22	Is deleted e-mail really gone?	13

Safe Shopping Online

Question 23	What questions should someone ask before making a purchase online?	14
Question 24	Who is the seller?	14
Question 25	What is the product?	15
Question 26	What are the legal terms of the purchase?	15
Question 27	How can privacy be maintained?	15
Question 28	How secure is the transaction?	16
Question 29	How should the item be paid for?	16
Question 30	When can delivery be expected?	16
Question 31	What records should be kept?	17
Question 32	To whom should complaints be made if something goes wrong with an online transaction?	18

Terms

Question 33	What is privacy?	19
Question 34	What is cyberspace?	19
Question 35	What is the Internet?	19
Question 36	What are online communications?	20
Question 37	What is e-mail?	20
Question 38	What is the World Wide Web?	21
Question 39	What is a newsgroup?	22
Question 40	What is chat?	22
Question 41	What is a cookie?	22

Sources & Bibliography

23

Graphs

		Page
Graph 1	Web Site Privacy Practices	2
Graph 2	Practices of Children's Web Sites	9
Graph 3	Family Rules for Computer Use	11
Graph 4	Internet Advertising Spending	14
Graph 5	Historical Milestones Leading to the Internet	19
Graph 6	Growth in Internet Web Sites	21

Tables

Table 1	Experienced Internet Users' Privacy Concerns	4
Table 2	Top Level Newsgroup Categories	6

Introduction

“The Information Highway will transform our culture as dramatically as Gutenberg’s press did the Middle Ages.”

— BILL GATES

The Internet — the information highway — is indeed revolutionizing our culture. The new technologies offer great opportunities, but at the same time could threaten our sense of privacy and basic civil liberties. This factbook serves as primer on basic questions about privacy in cyberspace. We examine questions raised by the government’s collection of personal data, the importance of privacy in our culture, children on the Internet, e-mail privacy in the workplace, and issues surrounding safe shopping online. This factbook is merely a sampling of some cyberspace privacy issues to help generate further reflection on how the information highway is changing our lives.

Sources of Information



Question 1 What information is collected by government agencies?

Answer The government collects a considerable amount of personal data on individuals. Drivers licenses and motor vehicle registration agencies collect information about a person's name, address, date of birth, Social Security number, physical description, make, model, and loan for automobile. Other information is collected on home ownership, land title, mortgage loans, and property taxes paid. Political registration and voting frequency

information is collected for voter registration purposes. Patient medical information is collected for various government agencies. Information about hobbies, such as hunting and fishing and boat and airplane ownership, is collected for licenses. Court records are also a major source of information because criminal matters, divorces and wills often place a wealth of personal details into the public domain.

Source: "Public Records, Public Policy and Privacy," Robert Gelman, *Human Rights*, Winter 1999, American Bar Association



Question 2 Is the information public?

Answer A public record is one maintained by law, regulation, or practice by or for a unit of government. The term "public record" implies that government records are necessarily in the public domain. This is true in terms of actions by legislative bodies, government agencies, court

decisions, and land ownership. Information collected about individuals is not necessarily in the public domain. For example, we do not make library loan records, criminal investigatory files, or welfare records public. The extent to which information is available varies among federal agencies, and from state to state.

Source: "Public Records, Public Policy and Privacy," Robert Gelman, *Human Rights*, Winter 1999, American Bar Association



Question 3 Are public records available online?

Answer Many government records are available online. Congress and federal agencies provide information about federal legislation and regulations online. Federal and state appellate courts publish opinions online. SEC filings are available online. State legislatures and executive agencies provide legislative information online. Other information is available online through

state and local government agencies. The American Bar Association web site provides links to many government and court sites through <http://www.abanet.org/lawlink/home.html>. LawLink™ also provides links to other legal organizations, bar associations, law schools, and other law related sites. Links to many government records can be found at law related web sites such as FindLaw.com or by contacting the agency directly.

Sources: "Public Records, Public Policy and Privacy," Robert Gelman, *Human Rights*, Winter 1999, American Bar Association; American Bar Association, LawLink™, <http://www.abanet.org/lawlink/home.html>



Question 4 What other information about people is available online?

Answer National phone books, mapping services that find individual addresses, and other directory services are online. More detailed personal information is also available online.

In recent years new industries have come into existence that profit from the personal data available from public sources as well as private computerized records. For example, these industries enable landlords to do online background searches on prospective tenants. In addition, credit report information is available online for businesses and others doing credit checks.

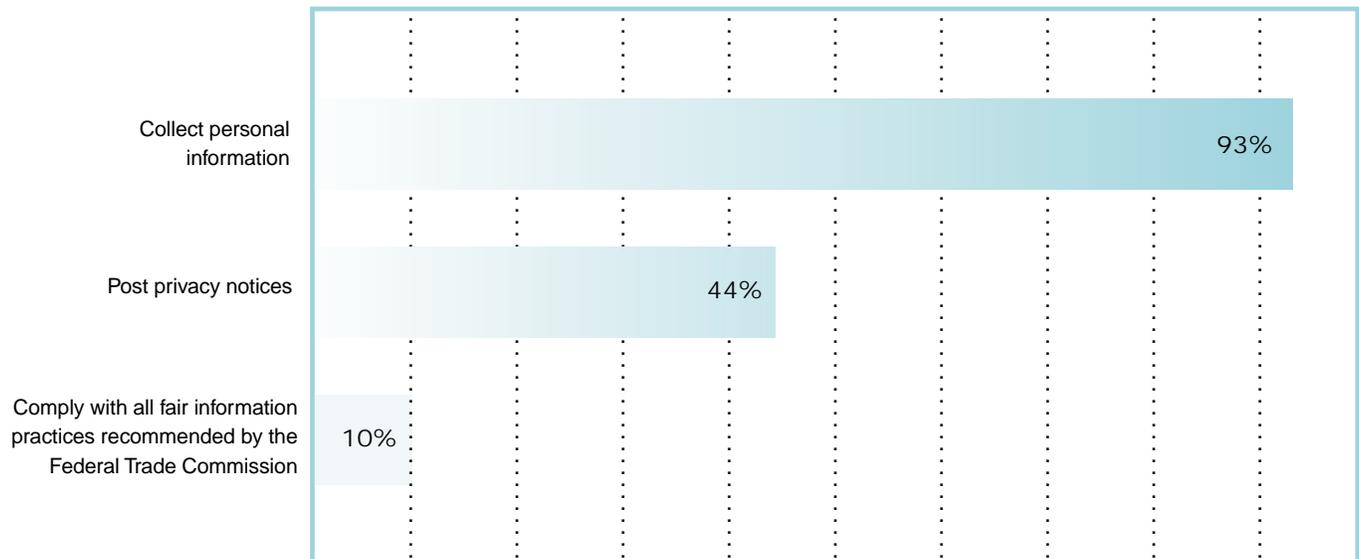
At least one company has advertised that it can provide the following information via e-mail in about

an hour: current and previous addresses going back 10 years, any additional phone numbers available, physical descriptions in Florida and Texas from drivers licenses, family members of individual, other people at same address, neighbors with listed phone numbers, spouses, summary of assets, professional licenses, property ownership and value, vehicle ownership and value, UCC lien filings, civil judgments, and bankruptcies.

A wealth of information is also collected from consumers visiting commercial web sites. Industry funded surveys have found the vast majority of commercial sites collect personal information from visitors to their sites.

Sources: "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission, July 1999; 1-800Search.com, <http://www.1800ussearch.com/home5.html>

Graph 1 / Web Site Privacy Practices



Source: Self-Regulation and Privacy Online: A Report to Congress, Federal Trade Commission, July 1999, citing Georgetown Internet Privacy Policy Survey.



The Importance of Privacy

 **Question 5** What can happen if someone's privacy isn't protected?

Answer A large amount of personal information about each of us is stored in various computers. Personal data can be used in identity theft or fraud. An imposter may create fake financial accounts and run up huge debts, or may simply appropriate someone else's finances.

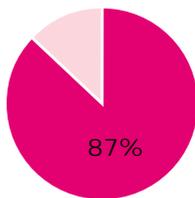
The ABA Division for Media Relations and Communication Services has created video news releases that demonstrate how consumer fraud on the Internet and identity theft can be a serious problem. The video news releases can be viewed on the ABA Media Relations web site, <http://www.abanet.org/media/lnn/home.html>

Other questions arise over possible use or misuse of data and whether this should be an area of greater legislative oversight. Personal data about medical conditions, family history, financial relationships, education, lifestyle,

shopping, and other habits is often stored and accessible through computers. For example, learning someone's Social Security number can be used as a starting point to collect large amounts of information about that person. The misuse of this information can embarrass, intimidate, or otherwise adversely affect individuals. This personal information might be used by employers, insurers, and others in ways individuals do not foresee or desire.

Eighty-seven percent of U.S. respondents to a 1999 survey of experienced Internet users stated they were somewhat or very concerned about threats to their privacy online. Another survey for the National Consumers League found 70 percent of the respondents uncomfortable providing personal information to businesses online.

Sources: "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission July 1999; "Cyberspace Privacy: A Primer and Proposal," Jerry Kang, *Human Rights*, Winter 1999, American Bar Association; "An Expert in Computer Security Finds His Life Is a Wide-Open Book," *New York Times*, <http://www.nytimes.com/library/tech/99/12/biztech/articles/13kirk.html>



Eighty-seven percent of experienced Internet users say they are concerned about threats to privacy online.

Source: "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission July 1999

 **Question 6** Why is this a particular problem in cyberspace?

Answer All cyberactivity, even simply browsing a web page, involves transmitting information that can identify you and be tracked. The data in cyberspace can be collected to produce telling profiles of what we do online and with whom we associate. The technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of us possible. One need only sift through the computer mouse clickstreams generated by our cyberactivity. Much of this information is detailed, computer processable, indexed to the individual, and permanent.

The 1999 Georgetown Internet Privacy Policy Survey reported information practices of 361 web sites drawn

from a list of 7,500 busiest servers on the World Wide Web. The survey found 93 percent of the sites collect personal information from consumers. Sixty-six percent provided at least one disclosure about their information practices. Forty-four percent of those sites post privacy notices. Only 10 percent of the sites are implementing all of the fair information practices recommended by the Federal Trade Commission and other government agencies. These would include notice of the information collected, consumer consent, access and ability to contest the accuracy of the information, and that information is secure from unauthorized use.

Sources: "Cyberspace Privacy: A Primer and Proposal," Jerry Kang, *Human Rights*, Winter 1999, American Bar Association; "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission, July 1999

Table 1 / Experienced Internet Users' Privacy Concerns

Unsolicited commercial e-mail is very serious	52%
Web sites collecting personal information from children is very serious	93%
Web sites collecting e-mail addresses from visitors without consent to compile e-mail marketing lists is very serious	80%
Tracking Web sites people visit and using that information improperly is very serious	87%
Very or somewhat concerned about threats to personal privacy while online	87%
Have personally been the victim of an online privacy invasion	19%
College and/or post graduate degree	48%
Send or receive e-mail	100%
Visit World Wide Web sites	100%
Have made online purchases	77%

Source: "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," AT&T Labs-Research Technical Report TR 99.4.3, April 1999, <http://www.research.att.com/projects/privacystudy>

Protecting Privacy

 **Question 7** Are there any laws governing dissemination of information collected by government entities and others?

Answer There are various legislative and court decisions restricting release of information. For example, income tax returns are not public information. Neither are criminal investigatory files or welfare records. The Driver's Protection Act (DPPA), a 1994 federal law (18 U.S.C. §2721) recently upheld by the Supreme Court, places prohibitions on states releasing most personal information gathered in the licensing process, with certain exceptions, or giving drivers the option to opt out of the release of the information for some purposes.

Earlier court decisions have held that federal agencies may withhold "rap sheets" — compilations of arrests, indictments, convictions or acquittals — on private citizens, even though the information is public at its original source, *Department of Justice v. Reporters Committee for Freedom of the Press*. Privacy concerns were cited in allowing federal officials to close records concerning refugees returned to Haiti, *Department of State v. Ray* (1991).

There are legal protections against invading privacy in various ways such as intrusion by wrongfully using

eavesdropping devices, publicizing private matters, publicizing in a false light, or appropriating a person's name or likeness for commercial purposes. The right to privacy can also be waived or relinquished in various ways such as consent, newsworthiness, and constitutional privilege. The privacy area of intrusion has generated a significant amount of concern within the media in defending a number of high profile cases in the 1990s.

Privacy is an area of growing concern for the media as it confronts First Amendment free press issues. Free!, the Freedom Forum's online publication, highlighted these concerns in December 1999 in a four-part series noting: "And it's the emergence of privacy — this right to be left alone — that has many journalists and news organizations pondering how press rights may fare in the years to come." In many cases, individual privacy is being balanced against the rights of a free press.

Sources: Free!, Freedom Forum Online, "Part One: Emergence of Privacy Rights Rattles Media," <http://www.freedomforum.org/press/series/1999/12/privacy.contents.asp>; "PART III Press advocates worry that privacy will trump First Amendment rights; <http://www.freedomforum.org/press/series/1999/12/28privacy3.asp>;" "PART IV Debate brews over balancing test between privacy and press rights;" "Public Records, Public Policy and Privacy," Robert Gelman, *Human Rights*, Winter 1999, American Bar Association; *Synopsis of the Law of Libel and Right to Privacy*, Bruce E. Sanford Second Revised Edition, Scripps-Howard Newspapers; First Amendment Center, http://www.fac.org/legal/supcourt/99-2000/reno_sum.htm

 **Question 8** How much privacy can someone expect when they are online?

Answer Few laws limit what the private sector can do with information collected in cyberspace. Unlike Europe, the United States has no omnibus bill covering the private sector's processing of personal information. There is a patchwork of laws regulating different types of information. There are numerous statutes covering con-

sumer credit, education, cable programming, electronic communications, videotape rentals, motor vehicle records, and the Children's Online Privacy Protection Act. However, in toto, information collectors can largely do what they want with most information collected in cyberspace. Commercial sites use this information to develop profiles of individual consumers to sell more effectively.

Sources: "We're Watching You, Tracking a Customer's Every Move is Key to Giving Marketers What They Want," R22, November 22, 1999, *Wall Street Journal*; "Cyberspace Privacy: A Primer and Proposal," Jerry Kang, *Human Rights*, Winter 1999, American Bar Association

 **Question 9** What are some clearly public activities?

Answer The government collects various information for the purpose of making it public. Campaign contribution statements and ethics statements from government officials are two examples. Some basic government functions and institutions rely on public availability of records to operate. The U.S. system of land ownership relies on the public availability of records. The public availability of bankruptcy records is also important.

Various online activities of individuals are clearly public activities, such as joining online chat rooms and newsgroups. Chat allows two or more computer users to “talk” to each other by typing in messages that are seen immediately by other parties to the “conversation.” Through an online newsgroup, conversations can take place on millions of

computers. The same conversation can be viewed and participated in by anyone with newsgroup access. Listservs are another mechanism where Internet users across the world can share information. With a single posting of a message, a Net user can distribute the message to all the users on the list around the world.

Sources: “Public Records, Public Policy and Privacy,” Robert Gelman, *Human Rights*, Winter 1999, American Bar Association; *The Internet Fact Finder for Lawyers*, Joshua Blackman with David Link, American Bar Association Law Practice Management Section (1998)

Table 2 / Top Level Newsgroup Categories

Identifier	Category	Example
biz	Business	biz.jobs.offered
comp	Computers	comp.ibm.software.microsoft.word
news	General news	news.announce.newusers
rec	Recreational	rec.games.chess
soc	Social	soc.rights.human
talk	Debate/Discussion	talk.environment
misc	Miscellaneous	misc.legal.computing
alt	Alternative	alt.business.import.export

Source: *The Complete Internet Handbook for Lawyers*, Jerry Lawson, ABA Law Practice Management Section (1999)

 **Question 10** Can online services and web sites access information stored on someone’s computer without their knowledge?

Answer Many web sites put “cookies” on computers that access the sites, which identifies the computer when it again comes to the site. With growing frequency, information about how consumers use the Web — the sites visited, search terms and other queries, online purchases, “click through” responses to advertisements — is being captured by advertising networks or “profiling companies.” With the permission of the Web site, but without seeking the consumer’s permission, these companies place a tag on the consumer’s computer. This tag — or identifier — is then used to track the consumer’s movements surfing the Web. In addition to long lists of collected information, a profile may contain “inferential” or “psychographic” data — information that the company infers about the consumer based on surfing habits. From this amassed

data, elaborate inferences may be drawn, including the consumer’s interests, habits, associations, and other traits.

Businesses that are concerned about these issues are attempting to self-regulate by joining organizations that attempt to control and disclose what information is collected. For example, TRUSTe is an industry-funded privacy organization with the responsibility of advising and overseeing Internet companies.

Concern over surreptitious collection of consumer data by Internet marketers and questionable distribution of that data has prompted members of both parties of Congress to call for more regulation of Internet companies. In January 2000, bills were also pending in California and New York to give consumers greater protection over the information collected by Internet service providers.

Sources: Center for Democracy and Technology, This Week’s Feature: Online Profiling Companies, <http://www.cdt.org>; cnn.com “Can TRUSTe protect users?” November 10, 1999; *Wall Street Journal*, “E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise,” A24, January 6, 2000



Question 11 How can people protect their privacy in cyberspace?

Answer There are various ways people can limit how much information is collected about them and limit the chances of others gaining access to information without their knowledge. One option is not to provide information that is not necessary, such as a Social Security number as an identifier, or credit card information to support a check. Others include:

PASSWORDS. Using a password can provide some security in cyberspace. However, computer hackers can readily use standard automated software to identify the password. To reduce the likelihood of that happening, one expert recommends that passwords be at least six characters long, contain a mix of alpha and numeric characters, and be changed regularly.

ELECTRONIC FOOTPRINTS. Users can visit web sites without revealing their identity by using a service that will conceal their identity, such as www.anonymizer.com or the Freedom system. E-mailing to unknown parties or posting to newsgroups or mailing lists can be done from a second e-mail account using a pseudonym. Many web sites, such as Yahoo and Excite, offer free e-mail accounts.

COOKIES. Some web sites are programmed to insert a small file onto the hard drive of a user's computer, so that the owner of the site can monitor where they go and what they do on the site. The site-owner might also be able to obtain an e-mail address. Netscape Navigator™ and Microsoft Internet Explorer® can be configured to warn a user when a site is attempting to deposit a cookie, and to allow the user to decide whether to accept it. It is also possible to buy software that will do the same thing.

SEAL PROGRAMS. Online seal programs are a way for consumers to find web sites that follow specified information practice. TRUSTe, a nonprofit organization founded by the CommerceNet Consortium and the Electronic Frontier Foundation, has more than 500 licensees representing a variety of industries. It requires licensees to follow certain standards for consumer notice, choice of information collected, access to the information, and security. BBBOnline, a subsidiary of the Council of Better Business Bureaus, launched its privacy seal programs for businesses in 1999. Several other seal programs have been developed.

Sources: *The Complete Internet Handbook for Lawyers*, Jerry Lawson, Law Practice Management Section, American Bar Association (1999); Safeshopping.org, <http://www.safeshopping.org/privacy/index.html>; Electronic Frontier Foundation, www.eff.org; "Privacy Tools Usher in Era of Net Anonymity," MSNBC, December 14, 1999, <http://www.msnbc.com/news/345954.asp?cp1=1#BODY>



Question 12 What is encryption?

Answer Encryption is a way of adding security to information that is transmitted over the Internet by scrambling the information so that it can't be understood by unauthorized persons. Modern encryption achieves greater security by using more secure algorithms and a concept known as public key encryption. The public key system uses dual keys, one public and one private. The fundamental principle of the system is that a message encrypted with either key can only be decrypted with the other key. The private key is kept secret. The public key

is usually widely available. If you encrypt mail using the recipient's public key, only someone knowing the private key should be able to read it.

Many web sites use Secure Sockets Layer (SSL) technology to encrypt credit card information that is sent over the Internet. These sites usually inform users whether they are using this technology. If the website begins with "https:" instead of "http:" this technology is in place. A different security technology, which works on different principles, is Secure Electronic Transaction, or SET technology. SET or SSL technologies are designed to make connections secure.

Source: Safeshopping.org, <http://www.safeshopping.org>



Question 13 How effective is encryption in ensuring privacy?

Answer Encryption provides an effective but not foolproof way of ensuring privacy. E-mail, for example, is most likely to be compromised from a person's own computer, whether in printing out e-mail messages, someone else opening the e-mail, or sending the message to the wrong person.

PGP®, or Pretty Good Privacy®, is a cryptographic product that enables people to securely exchange messages, and to secure files, disk volumes and network connections. Encrypting e-mail with PGP provides a high level of security if used correctly — the encrypted message can be read only by the intended recipient. However, PGP does not prevent the recipient from forwarding the message in an unencrypted form to others.

Many of the latest high-quality web browsers come from the manufacturer bundled with a form of encryption based on what is called S/Mime. These encryption mechanisms don't work automatically. Users purchase public-private key pairs from third parties such as Verisign or the U.S. Postal Service. In recent years, the domestic versions (128 bits) have been much more secure than the export versions (40 bits). In 1995, a French college student broke such software using two super-computers supplemented by about 100 powerful work stations. In 1993, a team of computer specialists working over the Internet broke a message with a key of 400 bits. Using about 1,000 powerful computers, it took a year.

Source: *The Complete Internet Handbook for Lawyers*, Jerry Lawson, Law Practice Management Section, American Bar Association (1999); *The Lawyer's Quick Guide to E-Mail*, Kenneth Johnson, American Bar Association Law Practice Management Section (1998)



Children on the Internet

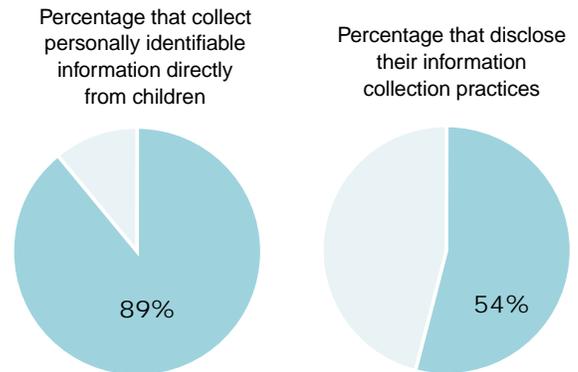
Question 14 How do web sites gather information about children?

Answer Many children are skilled navigators in cyberspace. About 42 million children are expected to be online by 2002. Advertisers and marketers are increasingly using the Internet to target children and gather information for marketing purposes. Such information can be obtained by asking children to register in order to play games, visit their favorite cartoon, or enter a contest. Web sites can also send e-mails to children as messages from their favorite action hero or cartoon character.

A 1998 Federal Trade Commission survey found that 89 percent of the 212 children's sites surveyed collect personally identifiable information directly from children; only 54 percent of the children's sites disclose their information collection practices.

Sources: SafeKids.com, Privacy Issues, <http://www.safekids.com>; "Children in Cyberspace," Beth Givens, *Human Rights*, Winter 1999, American Bar Association

Graph 2 / Practices of Children's Web Sites



Source: Federal Trade Commission survey (1998)

Question 15 Are there any laws regulating this?

Answer In 1997 the Federal Trade Commission issued broad principles that apply to the online collection of information about children. It defined as an "unfair practice" the collection and sale of personal information from children without due disclosure and parental consent. It covers such personal information as a child's name, phone number, address, or e-mail address.

In 1998, the Federal Trade Commission announced its first Internet privacy case, in which GeoCities, a developer of online publishing tools and communities, agreed to settle the Commission's charges that it misrepresented how it was using personal information collected from children and adults through its membership application and from registration forms for children's activities. The final settlement requires GeoCities to post a prominent privacy policy, to establish a system of parental consent

before collecting information from children, and to offer individuals from whom it had collected information an opportunity to delete the information.

In 1998, the Children's Privacy Protection Act was signed into law. It requires web operators with sites directed at children under 13 to provide notice to parents of their information practices; obtain prior, verifiable parental consent for the collection and use of personal information about their child; and limit what types of personal information are collected for participation in games. In October 1999 the Federal Trade Commission issued a final rule effective April 2000 implementing the law. The rule requires privacy notices on web sites, verifiable parental consent, parental choice in disclosure of information to third parties, safe harbor for industry groups engaged in self-regulation, and authorized the FTC to bring enforcement actions and civil penalties.

Sources: "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission, July 1999; "Children in Cyberspace," Beth Givens, *Human Rights*, Winter 1999, American Bar Association; Federal Trade Commission, <http://www.ftc.gov>

 **Question 16** Can web sites get around privacy laws by gathering information from cookies?

Answer Web sites can be designed to invisibly gather information about children's as well as adults' interests as they "travel" from web page to web page or site to site.

Moving from page to page often triggers the placement of "cookies" on the hard drive of the computer being used by the child, just as happens when adults move from site to site.

Source: "Children in Cyberspace," Beth Givens, *Human Rights*, Winter 1999, American Bar Association

"About 42 million children are expected to be online by 2002."

Source: Beth Givens, *Human Rights*, Winter 1999, American Bar Association

 **Question 17** What special risks do Internet chat rooms pose for children?

Answer Internet chat rooms, where children can communicate with each other in real time, are enormously popular with children. However, a 1996 Consumers Union survey found that one-third of children reported having problems with other chat room users. The most common problems were profanity, asking a user for his or her password, asking for personal information, inappropriate advances, and adults visiting chat rooms set aside for children.

Cyberstalking is a threat to users of online chat rooms, including children. One privacy group estimates there may be tens of thousands of cyberstalkers on the Internet.

Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity.

Sources: CyberAngels, How Prevalent is Cyberstalking?, <http://www.cyberangels.com/safetyandprivacy/stalk1.html>; SafeKids.com, "What Are the Risks?" http://www.safekids.com/child_safety.htm; "Children in Cyberspace," Beth Givens, *Human Rights*, Winter 1999, American Bar Association



Question 18 How can parents protect their children online?

Answer A number of products are available which, when installed on a personal computer, will block access to web sites containing objectionable material. These products include: NetNanny, CyberPatrol, CYBERSitter, and SurfWatch.

Some filtering products prevent access to a list of “bad sites.” Others can block access to the computer during specified hours of the day. Others provide parents with a log of web sites visited by their children. And some prevent access to services such as Internet chat rooms. None of these software programs has been proven entirely effective when put through a set of controlled tests. Critics of filtering software are also concerned about censorship of political, religious, social, or business viewpoints, or blocking legitimate non-obscene speech.

Some search engines also have developed their own search engines for children. Some example are:

- Ask Jeeves for Kids, <http://www.ajkids.com/>
- Yahoooligans, <http://www.yahoooligans.com/>
- OneKey, <http://www.onekey.com/live/index.htm>.

Ratings systems are another approach to reviewing web-based content. Apple computer has developed KidSafe, which specifies what kids see, rather than trying to filter out what they shouldn't see. KidSafe downloads a software module into the computer's operating system, which then verifies that each requested web destination is KidSafe by checking with Apple's KidSafe server.

In the final analysis there is no substitute for parental involvement in children's exploration of cyberspace.

Sources: SafeKids.com, <http://www.safekids.com>; The National Center for Missing & Exploited Children, <http://www.missingkids.com>; “Children in Cyberspace,” Beth Givens, *Human Rights*, Winter 1999, American Bar Association; Apple, <http://apple.com>

Graph 3 / Family Rules for Computer Use

The National Center for Missing & Exploited Children recommends family rules for computer use such as:

- ✓ Instructing children not to give out personal information online.
- ✓ Instructing children never to get together with someone they “meet” online.
- ✓ Check out web site blocking, filtering, and rating services.
- ✓ Instructing children not to respond to messages or bulletin boards that are suggestive, threatening or otherwise make the child uncomfortable.
- ✓ Setting time limits for a child's use of a computer.
- ✓ Making online use a family activity.
- ✓ Getting to know children's online “friends.”
- ✓ Explaining that people online may not be who they say they are.
- ✓ Learning about the online services a child uses.

E-mail Privacy in the Workplace

 **Question 19** Is there federal law covering e-mail privacy in the workplace?

Answer The Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2510-20; 2701-2711) prohibits unauthorized interception and accessing of e-mail, with fines up to \$10,000 and up to one year in prison. The law includes certain exceptions permitting e-mail service providers to intercept and access e-mail as part of an activity necessary in providing service. At least one court has ruled that the service provider exception to the law also applies to employers. There is also another exception in the law for employers whose employees consent to being monitored. An employee will likely be deemed to have consented by being aware of the employer's policy to monitor e-mail, and continuing to use e-mail.

If there is an improper use of an e-mail message intercepted by an employer, the employer might be exposed to liability. For example, if an employer fires an employee after learning from e-mail that he has AIDS or is taking medication for depression, the employee may have a claim under the 1990 Americans With Disabilities Act, which prohibits discrimination against people for various physical or mental impairments. Likewise, disciplinary actions against an employee based on information about an employee's physical disability, sexual orientation, social life, or other activities outside the workplace can be legal minefields. Both federal and state law come into play when employers use information about an employee gathered through e-mail monitoring.

Sources: Internet in the Workplace: Managing Organizational Access (1997), Software Publishers Association; "E-Mail in the Workplace: Limitations on Privacy," Mary E. Pivec and Susan Brinkerhoff, *Human Rights*, Winter 1999, American Bar Association

 **Question 20** Do state laws offer any protection to e-mail?

Answer Many states have adopted laws similar to the federal law protecting individual rights of privacy in electronic communication. Some states, such as Maryland and Florida, require the consent of both parties before an employer may monitor e-mail. Legislation in Virginia, Georgia, and West Virginia makes it illegal to use a computer or network to examine personal information without proper authority.

This is an evolving area of the law. Under these laws, there may be exceptions for employers to monitor e-mail

in the course of business. Nebraska permits employers to intercept e-mail in the normal course of business.

In many states, employees have little if any privacy protection from monitoring by employers. An increasing number of employers are monitoring and recording employee web usage, as well as e-mail. Some privacy groups suggest consumers keep private data and private net usage private by doing so from their own personal accounts from home personal computers.

Sources: Electronic Frontier Foundation's Top 12 Ways to Protect Your Online Privacy, <http://www.eff.org>; "E-Mail in the Workplace: Limitations on Privacy," Mary E. Pivec and Susan Brinkerhoff, *Human Rights*, Winter 1999, American Bar Association

 **Question 21** What about common law privacy?

Answer In the absence of legislation protecting employees, there may be actions against employers under common law tort law. The actions might be brought under the theory of tortious invasion of privacy. However, these suits will fail if the courts find the employees have no expectation of privacy or that their privacy is outweighed by other business interests of the employer. For example, a California court upheld the firing of employees of a car dealer for sending personal e-mail messages, *Bourke v. Nissan Motor Co.* YC 003979 Cal. Super. Ct., LA County (affirmed by the Court of Appeals in 1993). However, a Massachusetts court suggested that employees who were fired may have a right to privacy

because they had a measure of control by creating passwords and deleting e-mail from the system, *Restuccia v. Burk Tech* (LW No. 12-384-96 (Mass. Sup. Ct. 1996).

In *Smyth v. Pillsbury*, a federal court in Pennsylvania in 1996 held that an employer's interest in preventing inappropriate and unprofessional comments outweighed an employee's right to privacy. The court found that the employee had no reasonable expectation of privacy in the company e-mail system.

Many commentators state that employers can protect themselves by issuing a clear policy, or use of on screen reminders, or signed waivers that company e-mail is not private.

Sources: *Internet in the Workplace: Managing Organizational Access* (1997), Software Publishers Association; *E-Mail in the Workplace: Limitations on Privacy*, Mary E. Pivec and Susan Brinkerhoff, *Human Rights*, Winter 1999, American Bar Association

 **Question 22** Is deleted e-mail really gone?

Answer "Deleted" e-mail is often archived on tape and stored for years (deleting does not really delete). Backup copies may exist on either the sender's or recipient's personal computers or on the company's network. If the e-mail was sent through a commercial service or the Internet, it may have passed through several computers.

Each computer between the sender and the recipient may have kept a copy. Unlike postal mail, most e-mail is not really secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the e-mail is encrypted).

Source: *The Lawyer's Quick Guide to E-Mail*, Kenneth Johnson, American Bar Association Law Practice Management Section (1998)

Safe Shopping Online

Question 23 What questions should someone ask before making a purchase online?

Answer There are a number of questions that consumers should consider before shopping online. Who is the seller? What is the product? What are the legal terms of the purchase? How can privacy be maintained?

Answers to these questions will determine what legal rights and recourse consumers may have when shopping online. The ABA Section of Business Law has created a Safe Shopping web site, www.safeshopping.org, that provides helpful answers to many of these questions. Some of that information is summarized in the following section.

Source: Safeshopping.org, <http://www.safeshopping.org>

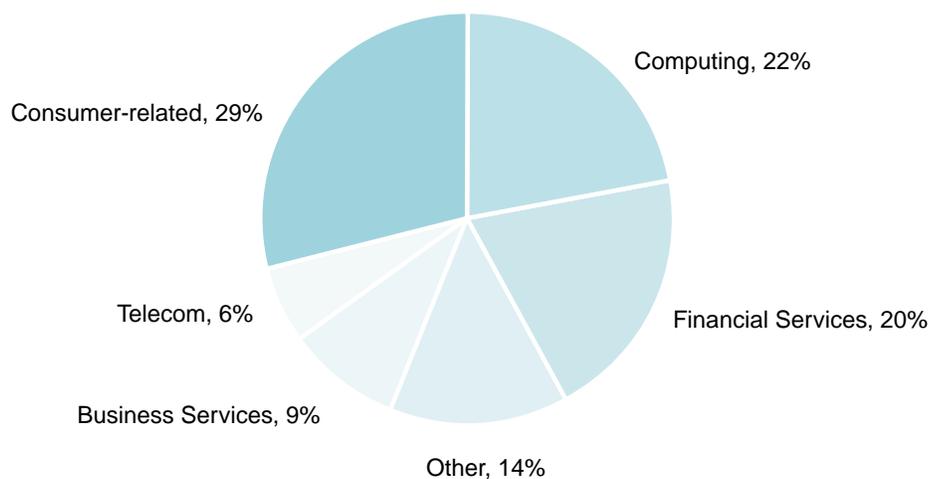
Question 24 Who is the seller?

Answer Does the seller regularly deal in the type of product you're interested in? Do they provide an address and phone number? Are they authorized to sell the product? If the seller is outside the United States, the consumer may not have the same legal rights as dealing with a company in the U.S.

Consumers may get better warranty service buying from an authorized seller. How do you know who's authorized? You can call the manufacturer of the product you're interested in, or visit the manufacturer's web site to check if the operator of the site has been authorized to sell the manufacturer's product.

Source: Safeshopping.org, <http://www.safeshopping.org>

Graph 4 / Internet Advertising Spending



Source: Internet Advertising Bureau

Question 25 What is the product?

Answer Is the product new or “refurbished?” Is it a brand name or a replica? Consumers should be suspicious of prices that appear too good to be true. Also consumers should consider if the price is too high, especially if through an auction house. It may be wise to comparison shop before buying online.

Many electronic order forms will tell you the total price of your order before you buy. Pay attention to that total price so you can crosscheck the items and quantity. Also, check any confirmation e-mail that you receive from the seller. If it doesn’t agree with what you wanted, immediately notify the seller by e-mail or telephone.

Source: Safeshopping.org, <http://www.safeshopping.org>

Question 26 What are the legal terms of the purchase?

Answer Is the seller offering or limiting warranties? How and where can an item be returned? Can an item be returned for cash, or only store credit? Who must be contacted to repair, replace or refund an item? Must the consumer mediate a dispute? Can the consumer sue in his or her home state?

A “full” warranty generally means that you’re entitled to free repair of the product during the warranty period, and do not have to pay shipping, removal, or re-installation costs. If the seller cannot fix the product

after a reasonable number of attempts, you’re entitled to a free replacement or full refund.

Any lesser warranty is “limited.” As you’d expect, there are more limited warranties than full ones. Nonetheless, they often provide substantial protection and value to a consumer. If a product is sold “as is” or “with its faults” that means the seller gives no warranty. If the seller “disclaims the implied warranty of merchantability,” that means the seller does not promise that the goods are fit for ordinary use. In some instances, the law provides that you must be given this warranty of fitness for ordinary use. Then a disclaimer isn’t effective.

Source: Safeshopping.org, <http://www.safeshopping.org>

Question 27 How can privacy be maintained?

Answer Web sellers are not yet required to respect privacy of information related to browsing their site. If the seller doesn’t have a privacy policy, consumers should consider whether to deal with that company.

A seller’s privacy policy should indicate:

- What information the seller is gathering from you
- How the seller will use this information, and
- Whether and how you can “opt out” of these practices.

Is the web site monitored by an independent organization? Although it may seem reassuring to find on a seller’s web site a logo, icon, or seal of an independent organization that monitors privacy policies and practices, consumers should also check the seller’s privacy policy. These organizations might not require the seller to adopt specific privacy practices. Instead, they might only require the seller to comply with whatever practices the seller has chosen to make part of its privacy policy. Nor is the independent organization necessarily financially liable if the seller breaches the terms of its privacy policy.

Source: Safeshopping.org, <http://www.safeshopping.org>

 **Question 28** How secure is the transaction?

Answer Did the consumer use a password? It is recommended to create different passwords for different web sites. If a site does not use a secure Internet connection, the consumer should carefully consider whether to give credit card information to the seller. Many encrypted sites indicate what security they are using.

Many web merchants allow consumers to order online and give credit card information over the phone. If you're more comfortable with this option, make a note of the phone number, company, the date and time of your call, and the name of the person who recorded your credit card number.

Source: Safeshopping.org, <http://www.safeshopping.org>

 **Question 29** How should the item be paid for?

Answer Paying by credit card is usually the safest way to pay. Under federal law, a consumer's liability for unauthorized charges made on a credit card is usually limited to \$50. Consumers may also be able to dispute the charges more effectively. The federal Fair Credit Billing Act provides some protections to consumers.

When it comes to other types of payment options such as debit cards, money orders, cashier's checks, certified checks, teller's checks, and cash on delivery (C.O.D.), consumers will find the level of protection isn't as high as with credit cards. Although there are pros and cons to these other payment options, using a credit card is still the best bet for safety.

Source: Safeshopping.org, <http://www.safeshopping.org>

 **Question 30** When can delivery be expected?

Answer U.S. law requires sellers to ship within the time promised in ads. If no date is promised, the item should be shipped within 30 days of receiving the order. The seller must notify consumers and give them the option to cancel if it can't meet the 30-day deadline.

Violating these rules or regulations can expose a seller to legal action by the FTC, the Postal Service, and state law enforcement authorities. The FTC can assess penalties of up to \$10,000 for each violation. These regulations do not apply to products ordered on a cash-on-delivery (C.O.D.) basis.

Source: Safeshopping.org, <http://www.safeshopping.org>

Question 31 What records should be kept?

Answer Consumers may want to keep hard-copy records of purchases and e-mail communication in case problems arise later. Such information should include a printout of the web pages indicating the sellers name,

postal address, and telephone number; a printout of the web pages describing the item(s) ordered; a printout of the web pages or pop-up screens that provide the sellers legal terms; and any e-mail messages discussing the product.

Source: Safeshopping.org, <http://www.safeshopping.org>





Question 32 To whom should complaints be made if something goes wrong with an online transaction?

Answer Check the site for a customer service page, “contact us” link, e-mail address, or phone number. Consumers with complaints should ask for what they think is fair — even if it’s more than the legal terms stated. A merchant isn’t forbidden from doing more than

required, if it will make the customer happy. If consumers are not satisfied with the answers or actions taken, they can contact the Better Business Bureau (<http://www.bbb.org>) or the Office of the State Attorney General in their state or the state where the seller is located, which can be accessed through the National Association of Attorneys General (<http://www.naag.org/find.htm>).

Source: Safeshopping.org, <http://www.safeshopping.org>

“As of the Third Quarter 1999, over 60 million people, or 69 percent of the online population, had shopped online in the past 3 months, representing an increase of over 15 million people from one year ago.”

Source: Worldwide Internet/Online Tracking Service, <http://www.intelliquest.com>

Terms

Question 33 What is privacy?

Answer Privacy has been defined as the quality of being apart from company or observation. It has also been described as freedom from unauthorized intrusion. Privacy can refer to a number of things such as a privacy right of an individual's persona, keeping information sent to others confidential, or concern over how data is collected on individuals and how it is used.

Most states by statute and judicial decision recognize that privacy can be invaded through unreasonably intruding upon the solitude or seclusion of others, publicizing a private matter, publicizing in a false light, or appropriating a person's name or likeness.

Sources: WWWebster Dictionary <http://www.m-w.com/cgi-bin/dictionary>; *Synopsis of Law of Libel and Right to Privacy*, Bruce E. Sanford, Second Revised Edition, Scripps-Howard Newspapers, ONLINE LAW (Addison Wesley, 1996, 1999).

Question 34 What is cyberspace?

Answer Merriam Webster's online dictionary defines cyberspace as "the on-line world of computer networks." Science fiction novelist William Gibson coined the word cyberspace in his book *Neuromancer* (1984), describing an

artificial environment created by computers, envisioned in realistic detail, in three dimensions and all five senses. Cyberspace today has come to be associated primarily with networks of computers linked through telephone lines.

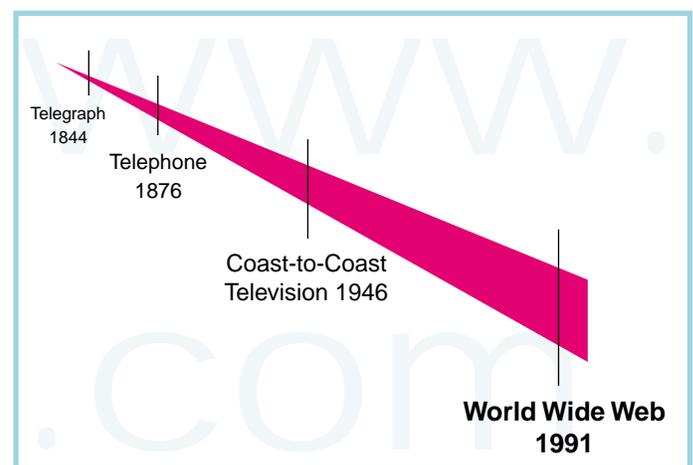
Sources: WWWebster Dictionary <http://www.m-w.com/cgi-bin/dictionary>; Encyclopaedia Britannica <http://www.britannica.com>, Year in Review 1995: computers-and-info-systems

Question 35 What is the Internet?

Answer The Internet is an electronic communications network that connects distinct computer networks and organizational computer facilities around the world. The Internet was developed in the 1970s to assist U.S. military and academic research. As recently as 1990, the Internet was almost unknown to the general public. By the middle of the decade, however, the network had absorbed millions of users with no affiliations to defense institutions or universities. It is estimated that almost 80 million adults in the U.S. are using the Internet.

Sources: WWWebster Dictionary <http://www.m-w.com/cgi-bin/dictionary>; "Self-Regulation and Privacy Online: A Report to Congress," Federal Trade Commission, July 1999

Graph 5 / Historical Milestones Leading to the Internet



Source: *The Complete Internet Handbook for Lawyers*, Jerry Lawson, American Bar Association Law Practice Management Section (1999)



Question 36 What are online communications?

Answer The phrase can refer to any communications over the Internet, typically through an online system. An online system is an electronic interactive system that delivers information to users via telephone lines or cables to personal computers (PCs) or terminals. The Internet can also be accessed via wireless and satellite based systems.

The Internet can be accessed in various ways. The first and most costly is to create your own Internet connection using a computer workstation and software and connecting via a high speed phone line such as a T1 line. A second means of connecting is through a commercial online service provider such as America Online. A commercial online service, often referred to as an Internet Service Provider (ISP), provides access to the Internet and also typically provides proprietary information about news,

education, business, entertainment, shopping, and more. Some also provide message services and graphic and audio information. A third prong of access is through an ISP that does not provide its own content but provides a pipeline to the Internet. The most common form of exploring the Internet is using a browser such as Netscape Navigator™ or Microsoft Internet Explorer®.

National and regional online systems usually have local telephone numbers that PC modems can call to access either a local information base or an indirect long-distance connection typically through a 28.8k or 56k modem. In recent years, consumers have increasingly turned to higher speed options such as cable modems (4 to 10 Mps) and digital subscriber lines (up to 1.5 Mps) to view video and graphics more readily over the Internet.

Sources: Encyclopaedia Britannica <http://www.britannica.com>; *The Internet Fact Finder for Lawyers*, Joshua Blackman with David Link, American Bar Association Law Practice Management Section (1998)



Question 37 What is e-mail?

Answer E-mail is electronic mail. Messages can cross the globe in a few seconds to a few hours. It is usually free as part of a normal monthly online service. E-mail typically requires an e-mail account from which to send and receive messages, and an e-mail program to create and read messages. Most current e-mail programs have standard features including: an address book to store names and addresses, replying with the text of the

original message, storing sent messages, forwarding messages, saving messages in folders, filtering messages, and attaching files to messages. The computer sending the mail and the computer receiving the mail do not need to be connected. The mail is passed from one computer to another until it reaches its destination. Each of the intermediary computers temporarily stores the message before sending it on to the next computer.

Source: *The Lawyer's Quick Guide to E-Mail*, Kenneth Johnson, American Bar Association Law Practice Management Section (1998).



Question 38 What is the World Wide Web?

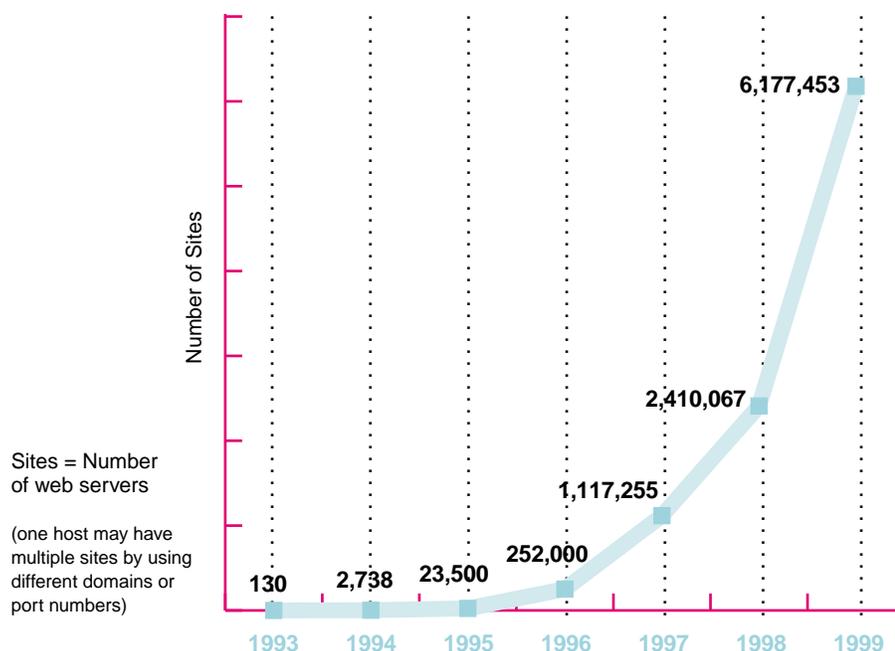
Answer In 1991, The World Wide Web (www) was developed by CERN, the European Laboratory for Particle Physics and developer Tim Berners-Lee. It revolutionized the Internet. It uses the “hypertext” model, where documents — web pages — are connected to each other via links. Each hypertext document can contain links to other pages on the same site or to pages on computers across the world. To access the web, users run graphical based browser programs such as Netscape Navigator™ or Microsoft Internet Explorer®. Through pointing and clicking on links, users can access text,

video, and other information from web pages anywhere on the Internet.

Public access to the web continues to grow at an astounding rate. The Internet reached an important milestone in October 1999 when an average of 1 billion hits (web pages viewed) per day were recorded in the United States. The report from online measurement service Media Metrix Inc., which tracks cyber traffic at home and at work, recorded 32.2 billion page views in October. That traffic report, which was a record, was up 49 percent from the same period in 1998.

Sources: *Law, Law, Law on the Internet*, Erik J. Heels and Richard P. Klau, American Bar Association Law Practice Management Section (1998): “A Net Record: 1 billion page views per day,” November 22, 1999 ZD Netnews, <http://news.excite.com/news/zd/991122/16/a-net-record>; Hobbes Internet Timeline© v. 4.2, <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>

Graph 6 / Growth in Internet Web Sites
June 1996 – June 1999



Source: Hobbes Internet Timeline©, 4.2, <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>

 **Question 39** What is a newsgroup?

Answer A newsgroup is an electronic bulletin board on the Internet devoted to a particular topic. There are thousands of such newsgroups available, on practically any conceivable topic. Internet newsgroup conversations can take place on millions of computers. The same

conversation can be viewed by anyone with access to the newsgroup. Participants can pose questions to which others can respond. An easy way to read newsgroup articles on a particular subject is via DejaNews, www.dejanews.com. This site provides an intuitive search engine type window on newsgroup content.

Source: *The Internet Fact Finder for Lawyers*, Joshua Blackman with David Link, American Bar Association Law Practice Management Section (1998)

 **Question 40** What is chat?

Answer A chat group is part of a system that allows two or more computer users to “talk” to each other by typing in messages that are seen immediately by other parties to the “conversation.” The Internet’s version is called IRC, Internet Relay Chat. Chat features are being built into interactive web sites and Internet conferencing

programs. Many proprietary programs are available as well, such as AOL Instant Messenger. Voice chat is also available, allowing users to speak to each other over the Internet. Some web sites feature chat rooms as a way to build a sense of community among users in a hope of drawing repeat visitors. More information about chat is available at <http://www.icq.com>.

Source: *The Complete Internet Handbook for Lawyers*, Jerry Lawson, Law Practice Management Section, American Bar Association (1999)

 **Question 41** What is a cookie?

Answer A cookie is information stored on the user’s computer that identifies the user visiting a web site. Web sites can use this information in many ways including developing profiles on visitors to their sites

and information they seek. Netscape Navigator™ keeps this information in a text file called Cookies.txt in the Navigator directory. Netscape Navigator and Microsoft Internet Explorer® browsers have privacy settings that can be adjusted to warn users before accepting cookies.

Source: Encyclopaedia Britannica <http://www.britannica.com>; Safeshopping.org, <http://www.safeshopping.org>

Sources & Bibliography

PUBLICATIONS

Blackman, Joshua and David Link, *The Internet Fact Finder for Lawyers*, American Bar Association Law Practice Management Section (1998)

"E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise," *Wall Street Journal*, A24, January 6, 2000

Federal Trade Commission, "Self-Regulation and Privacy Online: A Report to Congress," July 1999

Gelman, Robert, "Public Records, Public Policy and Privacy," *Human Rights*, Winter 1999, American Bar Association

Givens, Beth, "Children in Cyberspace," *Human Rights*, Winter 1999, American Bar Association

Heels, Erik J. and Richard P. Klau, *Law, Law, Law on the Internet*, American Bar Association Law Practice Management Section (1998)

Internet in the Workplace: Managing Organizational Access (1997), Software Publishers Association

Johnson, Kenneth, *The Lawyer's Quick Guide to E-Mail*, American Bar Association Law Practice Management Section (1998)

Kang, Jerry, "Cyberspace Privacy: A Primer and Proposal," *Human Rights*, Winter 1999, American Bar Association

Lawson, Jerry, *The Complete Internet Handbook for Lawyers*, American Bar Association Law Practice Management Section (1999)

Pivec, Mary E. and Susan Brinkerhoff, "E-Mail in the Workplace: Limitations on Privacy," *Human Rights*, Winter 1999, American Bar Association

Sanford, Bruce E., *Synopsis of the Law of Libel and Right to Privacy*, Second Revised Edition, Scripps-Howard Newspapers

WEB SITES

"A Net record: 1 billion page views per day," November 22, 1999, ZD Netnews, <http://news.excite.com/news/zd/991122/16/a-net-record>

American Bar Association, LawLink™, <http://www.abanet.org/lawlink/home.html>

"An Expert in Computer Security Finds His Life Is a Wide-Open Book," *New York Times*, December 13, 1999, <http://www.nytimes.com/library/tech/99/12/biztech/articles/13kirk.html>

"Can TRUSTe protect users?" November 10, 1999, <http://www.cnn.com>

Center for Democracy and Technology, This Week's Feature: Online Profiling Companies, <http://www.cdt.org>

Electronic Frontier Foundation, <http://www.eff.org>

Encyclopaedia Britannica <http://www.britannica.com>

Federal Trade Commission, <http://www.ftc.gov>

First Amendment Center, http://www.fac.org/legal/supcourt/99-2000/reno_sum.htm

Free!, "Part One: Emergence of Privacy Rights Rattles Media," Freedom Forum Online, <http://www.freedomforum.org/press/series/1999/12/privacy.contents.asp>

Free!, "Part III: Press Advocates Worry That Privacy Will Trump First Amendment Rights," Freedom Forum Online, <http://www.freedomforum.org/press/series/1999/12/28privacy3.asp>

Free!, "Part IV: Debate Brews Over Balancing Test Between Privacy and Press Rights," Freedom Forum Online, <http://www.freedomforum.org/press/series/1999/12/29privacy4.asp>

Hobbes Internet Timeline © v. 4.2, <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>

WEB SITES (continued)

“How Prevalent is Cyberstalking?” CyberAngels,
[http://www.cyberangels.com/safetyandprivacy/
stalk1.html](http://www.cyberangels.com/safetyandprivacy/stalk1.html)

National Center for Missing & Exploited Children,
<http://www.missingkids.com/>

“Privacy Issues,” SafeKids.com, <http://www.safekids.com>

“Privacy Tools Usher in Era of Net Anonymity,” MSNBC,
December 14, 1999, [http://www.msnbc.com/news/
345954.asp?cp1=1#BODY](http://www.msnbc.com/news/345954.asp?cp1=1#BODY)

Safeshopping.org, <http://www.safeshopping.org>

“We’re Watching You, Tracking a Customer’s
Every Move is Key to Giving Marketers What They
Want,” *Wall Street Journal*, R22, November 22, 1999

“What Are the Risks?” SafeKids.com,
http://www.safekids.com/child_safety.htm;

Webster Dictionary [http://www.m-w.com/
cgi-bin/dictionary](http://www.m-w.com/cgi-bin/dictionary)

1-800Search.com [http://www.1800ussearch.com/
home5.html](http://www.1800ussearch.com/home5.html)

