Security and Privacy of Information Belonging to Children and in Educational Records

CHAPTER 5

SEVERAL LAWS ARE IN PLACE in the United States to protect children when they are online. The Children's Online Privacy Protection Act (COPPA) governs how information from children is to be collected and used. If you host a Web site that collects information from children, COPPA applies to you. The Children's Internet Protection Act (CIPA) protects minors from obscene or objectionable material on school or library computers. These computers must implement technology to filter objectionable content. The Family Educational Rights and Privacy Act (FERPA) protects the privacy rights of students and their educational records. Students and parents have the right to review these records. Additionally, schools cannot release records without the written consent of a student or parent.

This chapter begins with a discussion of children and the Internet, and the unique challenges Web site operators face in protecting children. The chapter then provides details about COPPA, CIPA, and FERPA.

Chapter 5 Topics

This chapter covers the following topics and concepts:

- What challenges exist in protecting children on the Internet
- What the Children's Online Privacy Protection Act (COPPA) is
- What the Children's Internet Protection Act (CIPA) is
- What the Family Educational Rights and Privacy Act (FERPA) is

Chapter 5 Goals

When you complete this chapter, you will be able to:

- List some of the challenges with protecting children on the Internet
- Identify the purpose and scope of COPPA, and describe its main requirements and oversight responsibilities
- Identify the purpose and scope of CIPA, and describe its main requirements and oversight responsibilities
- Identify the purpose and scope of FERPA, and describe its main requirements and oversight responsibilities

Challenges in Protecting Children on the Internet

U.S. children ages 8 to 18 spend over seven hours a day using electronic media. This includes television, music, computer use, and video game use.[1] Parents, schools, and Web site providers all have different roles to play in protecting children when they are online. It's not unusual to hear about cases where Web site operators run afoul of the laws that attempt to protect children:

- In 2013, a social media company paid $800,000 to settle charges with the Federal Trade Commission (FTC). The company had an app that allowed children to create journals and share those journals online. Children could also post photos and share location information. The FTC alleged that the company violated the Children's Online Privacy Protection Act (COPPA). The company collected the birth dates of 3,000 children before getting parental permission.
- A company that created virtual online gaming worlds agreed to pay $3 million in 2011 to settle charges with the FTC. The FTC alleged that the company improperly collected and disclosed the personal information of thousands of children without parental consent. This is the largest civil penalty so far in a COPPA action.
- A student sued a local school board alleging that the school had violated the student's First Amendment rights. The lawsuit alleged that the school's Internet filtering software blocked too much legitimate content. In this case, computers in the school library blocked access to Web sites that promoted gay rights, but allowed access to Web sites that opposed gay rights. The student did not challenge that federal law required the school to use filtering software to block obscene material. In 2012, a federal court judge found that the school's blocking software configuration was unconstitutional. It ordered the school to reconfigure its software to make sure that did not discriminate against different viewpoints.

Although most people agree that children should be protected when they are online, they don't always agree on how that should be accomplished. For example, some people suggest that a parent should monitor a child's Internet access and decide if the child's Internet activities are acceptable. Others suggest that laws should be in place to protect the child even if a parent is not monitoring the child's Internet use. As you will see in this chapter, several laws have been enacted to protect children. Most of these laws are directed at the Web site operators who provide online content to children.

However, even when enacting laws, challenges still exist. These include:

- **Identification of children**—How can Web site operators distinguish between adults and children online?
- **First Amendment and censorship**—When does censoring certain types of content violate the First Amendment?
- **Defining objectionable content**—Where is the dividing line between material that is merely inappropriate for children and that which is truly objectionable?

Identification of Children

In 1993, the *New Yorker* published the now-famous cartoon by Peter Steiner with the caption, "On the Internet, nobody knows you're a dog." It is just as hard to separate children from adults on the Internet. To protect children, you must be able to identify them. Although you can require identification from restaurant customers to ensure they're old enough to purchase alcohol, it isn't easy to require identification when users access a Web site. Most users can easily remain anonymous when they're online. This creates a problem for Web site operators. Most of the laws that aim to protect children while they are online require Web site operators to be able to distinguish children from adults.

Web site operators can use several methods to distinguish children from adults. These include:

- **Requiring user input**—A Web site can require users to identify if they are children or adults. For example, users can select a check box indicating they are over a certain age. They can be required to enter an age or a birth date. This isn't a foolproof method, however, because people can simply lie about their age. If a child accesses an age-restricted Web site under false pretenses, the Web site operator can still be liable for providing objectionable content to a child.
- **Requiring payment**—If a Web site has material that should be restricted from children, it can require a payment to access the site. Payment can be made using a credit card, a PayPal account, or another method that a child is unlikely to be able to use. The payment may be a nominal fee, such as 99 cents. It could also be a larger fee designed to generate revenue. A payment requirement can be effective because children generally don't have access to means of payment.

> **NOTE**
>
> The Entertainment Software Rating Board (ESRB) is a self-regulating nonprofit that assigns independent ratings to computer and video game content. This includes games available online. The ratings help parents select appropriate games and other content for their children. Web site operators can rate their Web sites according to ESRB so that parental controls work properly. Visit *http://www.esrb.org* to learn more.

- **Using parental controls**—Some operating systems include parental controls. So do many applications. **Parental controls** allow a parent to restrict their children's access to objectionable material based on different ratings.
- **Requiring parental consent**—If a child wishes to access a particular Web site, that site can block the child's access until a parent provides permission. This means that the Web site operator implements controls to verify that a parent is providing consent to access the Web site.

First Amendment and Censorship

The First Amendment is a part of the Bill of Rights. The First Amendment grants certain rights related to freedom of speech. It also protects freedom of the press and the free exercise of religion. First Amendment issues come into play on the Internet in many different ways:

- Individuals online have a First Amendment right to view lawful content, including content that others might find troubling.
- Web site operators and other content creators have a First Amendment right to post lawful content, including content that others might find troubling.

The U.S. Supreme Court has said that the right to freedom of speech applies to the Internet.[2] This means that the government can't restrict an adult's access to content on the Internet. However, the government can restrict a child's access to harmful online materials if the government has a compelling reason to do so.

When the government restricts a child's access to objectionable online materials, other issues are raised. Does it violate a Web site operators rights to force it to censor material because a child might view it? If individuals are required to identify themselves before they can use a Web site, such as proving that they're not children, does that restrict their free speech? Does it restrict free speech if individuals are required to identify themselves by name in comments on a Web site? If libraries are required to use filters on computers to keep children from viewing objectionable content, does it restrict the free speech rights of adults who also use those computers?

Many of these issues continue to evolve within the context of the laws discussed in this chapter.

Defining Obscenity

The laws discussed in this chapter protect the privacy of children. They protect children from harmful content. For the most part, this harmful content is content that would be considered obscene. Most people agree that children should not see obscene material. However, it is difficult to legally define what obscene material is.

I Know It When I See It

A 1964 U.S. Supreme Court case shows the difficulty of defining obscenity.[3] In *Jacobellis v. Ohio*, a movie theater manager was convicted under state law of illegally possessing and exhibiting an obscene film. The state supreme court upheld the conviction. The U.S. Supreme Court later reversed that decision.

In this case, the Court agreed that the First Amendment does not protect pornography or obscenity. It disagreed about whether the motion picture was obscene. In the Court's decision, Justice Potter Stewart expressed the difficulty of defining what is obscenity and pornography. He wrote "But I know it when I see it, and the motion picture involved with this case is not that."

This case was decided over 50 years ago. Yet the challenge of identifying obscenity still exists today.

The U.S. Supreme Court addressed this in 1973. In *Miller v. California* the Court said that for material to be identified as "obscene," it must meet three conditions. The conditions are based on the average person applying contemporary community standards to a review of the material. The three conditions are that the material:

- Appeals predominantly to prurient interests—*prurient* indicates a morbid, degrading, and unhealthy interest in sex
- Depicts or describes sexual conduct in a patently offensive way
- Lacks serious literary, artistic, political, or scientific value[4]

NOTE

The three conditions for defining obscenity are known as the *Miller* test.

It isn't always easy to apply this definition. What one person considers obscene, another person may consider healthy. Material that one person finds informative may be deemed tasteless by another. Material that is offensive to one person may be viewed as valuable by another. How a person views material is often influenced by societal, family, community, and religious values.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA)[5] passed in November 1998. It first went into effect in April 2000. COPPA governs how Web sites collect information from children under the age of 13. The Federal Trade Commission (FTC) oversees COPPA compliance. It has the power to make rules for COPPA compliance. The FTC Rule governing COPPA is called the *COPPA Rule*. This rule was first drafted in 1999. In 2012 the FTC revised the rule to respond to changes in technology. The new rule gives parents more control of how their children's information is used. The revised rule went into effect in July 2013.

> **NOTE**
>
> COPPA is not the same as the Child Online Protection Act (COPA). COPA was enacted in 1998. Its purpose was to protect minors from access to harmful material on the Internet. However, courts ruled that COPA violated free speech and the law never went into effect. CIPA is similar to what COPA attempted to accomplish and is discussed later in this chapter.

Web sites must follow specific rules under COPPA to collect and use information from children. There are several important definitions in the COPPA Rule:

- **Child**—Any person under the age of 13
- **Parent**—The legal guardian of a child
- **Operator**—A Web site operator, or operator of an online service, who collects or maintains personal information about users

Purpose of COPPA

The primary purpose of COPPA is to protect children's privacy on the Internet. Web sites must follow specific rules if they collect or use a child's personal information. They must obtain a parent's consent before doing so. They must also post a privacy policy explaining their practices.

Personal information includes:

- A child's first and last name
- A child's e-mail address or other online contact information such as an Instant Messaging username or voice over internet protocol (VOIP) identifier
- A child's screen name or username
- A child's physical address, such as their home address
- A child's telephone number
- A child's Social Security number
- Photographs, video, or audio files that contain a child's image or voice
- Geolocation data that identifies a physical address
- Any persistent identifier, such as an Internet cookie or Internet Protocol (IP) address that is used to recognize a user over time and across different Web sites
- Any other information concerning a child or the child's parents that a Web site operator collects from a child and combines with any other data about a child[6]

Any personal information that's collected must be protected. This means that the Web site operator must protect the confidentiality, security, and integrity of this data. Web site operators must ensure the information isn't made publicly available to others. This includes making sure it isn't displayed on a home page of a Web site, on a message board, or in a chatroom. The law allows Web site operators to share this kind of data only for specific reasons. However, when Web site operators share this information, they must share it only with third parties who can properly protect it.[7]

Scope of the Regulation

COPPA applies to anyone operating online services that collect or use information about children under the age of 13. This includes situations where the Web site operator directly collects the information. It also includes situations where the Web site operator lets third parties collect the information. Even general-audience Web sites might have to follow the COPPA Rule. If operators of such sites know they are collecting data from children, then they must comply with COPPA. An operator might know that its site is collecting data from children if it asks users to share their birth date. An operator that collects demographic data such as school attendance and grade completion might also know that children are using its Web site.

The definition of Web site or online service is broad. It includes standard Web sites. It also includes:

- Mobile apps
- Internet gaming platforms
- Advertising networks[8]

Main Requirements

COPPA has two main rules that Web sites must follow in order to comply with the rule. Operators must:

- Post a privacy policy
- Get verifiable parental consent before collecting information from children

Privacy Policy

Under COPPA, Web sites must post a privacy policy.[9] The privacy policy states the kind of information the site collects about children. It also states how the site will use the information. The COPPA Rule tells operators the terms that must be included in the privacy policy.

COPPA requires that a Web site privacy policy should be easily visible and accessible. The rule requires that a link to the privacy policy be included on the home page of the Web site. The rule also requires that the link be posted on every area of the Web site where a child's personal information is collected.[10] A COPPA-compliant privacy policy must be accessible from a clear and prominent link. This means the link needs to stand out and be noticeable. A Web site designer can achieve this in a variety of ways. For example, the designer can use different type sizes, fonts, colors, or contrasting backgrounds to highlight the link. In addition, the privacy policy must be clearly labeled to indicate it's a privacy policy. The most common label is "Privacy Policy." Other examples of clear labels are "Privacy Statement" and "Information Practices Statement."

> **NOTE**
>
> COPPA doesn't specifically use the phrase "privacy policy." It requires Web site operators to provide a notice on their Web sites that identifies the collected information. However, the FTC's COPPA Rule calls this notice a "privacy policy."

Privacy Policy Content

The privacy policy needs to contain specific information to be COPPA-compliant. It must be clearly written and easy to read. The format isn't as important as the content. At a minimum, the policy must contain:

- **Operator contact information**—This includes the name, mailing address, telephone number, and e-mail address of all operators collecting or using the information collected on the Web site. If several operators are collecting information, the policy can list the contact details for only one operator under two conditions. First, the names of all operators must be listed in the privacy policy or in a link accessible from that policy. Second, the listed operator must respond to all questions about the policy. It also must answer questions about how data is collected and used on the site.
- **Notice of what information is collected**—The policy must be specific. A generic term such as "contact information" isn't acceptable. Instead the policy should specify child's name, address, telephone number, gender, age, and e-mail address.
- **Notice of how information is collected**—A Web site can collect information actively or passively. A user entering information into a form is active collection. A Web cookie that collects personal information is passive collection. The privacy policy must clearly state how information is collected.
- **Notice of how the information will be used**—Web sites must state how the information will be used. It must be specific. For example, a Web site could collect e-mail addresses for newsletter subscriptions. It could collect mailing addresses for prizes. It could also collect the information for sales and marketing purposes. Each use must be clearly stated.
- **Notice of whether the information is disclosed to third parties**—The Web site must also state whether collected information is shared with a third party. These are any entities that aren't the operator of the Web site. Third parties also include entities that don't provide internal support for the Web site. Parents may refuse to share the collected data with third parties.
- **Assurance that participation is not conditioned on data collection**—That is, a Web site can't require children to submit contact details in order to be allowed to use the site. Web sites are not allowed to collect more information than necessary for a child to participate in an activity. This prevents the Web site from collecting too much information about a child. For example, a Web site may collect an e-mail address for an online newsletter subscription. Collecting a physical mailing address for an online newsletter is not reasonable. The privacy policy should clearly state that a Web site won't condition participation on information collection.

- **Parental rights**—The policy must state that a parent can review information collected on his or her child. Parents can also tell the Web site to delete any data it has collected. Parents can also refuse further data collection. They can also refuse to allow the Web site to share collected information with third parties.

> **NOTE**
> There are many Web sites directed toward children. Next time you visit one of them, see if you can find the Web site's privacy policy. Is it easy to find? Does it contain the terms discussed in this section?

Gaining Parental Consent

COPPA has specific rules about getting parental consent. This consent is required if a Web site wants to use and collect data from a child. Web site operators must take reasonable steps to make sure that a parent receives direct notice of the operator's data collection practices. This notice must include:

- That the operator has collected the parent's online contact information from the child in order to obtain parental consent
- That the parent's consent is required to collect, use, or disclose the child's information. The notice must state that the operator will not collect, use, or disclose the child's information without parental consent
- The specific items of data that the Web site operator wants to collect from the child
- A link to the Web site privacy policy
- How the parent can give verifiable consent to the collection, use, and disclosure of the child's information
- That if the parent does not provide consent within a reasonable time, the operator will delete the parent's online contact information from its records[11]

Under COPPA, parental consent must be verifiable. Only a parent can give consent. A Web site operator must verify the identity of the parents that it contacts. This becomes especially important if the parent requests to see the information held about his or her child. Web site operators must have measures in place to prevent the information from being released to the wrong party.[12]

Parents have other rights under the COPPA Rule. The Web site must re-notify parents whenever it changes its data collection and use procedures. Parents must be allowed to review information collected from their children. They also must also be allowed to revoke their consent. If a parent revokes his or her consent, Web site operators must stop collecting, using, or disclosing that data immediately. Parents also can request that a Web site operator delete data held on their children. Web site operators must make parents aware of how to exercise these additional rights.

Consent is not required at all in some instances. Web sites don't need parental consent if they're collecting an e-mail address to respond to a one-time request from a child. Nor do they need consent to provide the initial notice to the parent. Consent is also not required to collect a child's name and online contact information to protect the security of the Web site.

Verifying Parental Consent

A Web site operator can use one of several methods to verify a person is a parent of a child and get consent for data collection. These include:

- **Sending signed printed forms**—These may be sent via mail, fax, or e-mail. An electronic scan of a signed consent form is permissible.
- **Provide government-issued identification**—Parents can provide copies of government-issued ID that can then be checked against a database. In this situation, Web site operators must delete the identification record once the verification process is completed.
- **Using credit cards or other online payment forms**—The credit card or online payment mechanism can verify details about the parent.
- **Using toll-free numbers**—Parents can call and provide details to verify their identities.
- **Using video conference**—Parents can connect via video conference to trained personnel in order to provide details to verify their identities.

Some operators suggest that these methods are too costly to be practical. As a result, many Web sites try to avoid the law. They don't collect information on children, and their privacy statement reflects this. Users are required to indicate they are at least 13 years old before information is collected. Users must enter their age or check a box indicating they're at least 13 years old. However, it's possible for children to indicate they're over 13 years old when they are not.

In some instances, upfront consent is not required. In these special circumstances the Web site must still later tell parents that it collected data. For example, a Web site can collect a child's name, parent's name, and online contact information in order to protect a child's safety. If a Web site collects this information, it must later tell parents that it collected the information and it must not use this information for any other purpose.[13]

NOTE

The FTC summarizes the COPPA Rule at *http://www.business.ftc.gov/privacy-and-security/childrens-privacy*.

Oversight

The FTC provides oversight for COPPA. The FTC investigates complaints of Web sites that violate COPPA. It can also bring enforcement actions and impose civil penalties for COPPA violations. The FTC provides many tools to help Web site operators comply with the law.

Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA)[14] passed in 2000. It requires schools and libraries that receive funding from the U.S. government for Internet access to filter offensive and sexually explicit online content. These schools and libraries had until July 1, 2004, to first comply with CIPA. The goal of CIPA is to limit children's access to offensive content on the Internet. Under CIPA, a minor is anyone under the age of 17.[15]

CIPA was quickly challenged. The American Library Association and the American Civil Liberties Union sued the U.S. government. They claimed CIPA violated the free speech rights of adults. They also claimed the law was so broad that it could prevent minors from getting information about topics such as breast cancer. In 2002 the U.S. District Court for the Eastern District of Pennsylvania agreed that CIPA violated First Amendment rights. The U.S. District Court said that the government could not enforce CIPA. The U.S. government appealed that decision.[16]

The suit went to the U.S. Supreme Court. In *United States et al. v. American Library Association, Inc. et al.* in 2003, the U.S. Supreme Court overturned the District Court ruling and upheld the law. The Supreme Court said that the law was constitutional because it was conditional. That is, only schools and libraries that chose to receive federal funding to subsidize their Internet access costs were required to follow the law. If it wanted to, a school or library can choose not to accept the funding. If a school or library chose not to accept the funding, then it did not have to comply with CIPA.

NOTE

Note the differences in ages between CIPA and COPPA. COPPA defines a child as anyone under the age of 13. CIPA defines a minor as anyone under the age of 17.

Purpose

The primary purpose of CIPA is to protect minors from accessing offensive content on the Internet. Offensive content includes any visual depictions that are any of the following:

- Obscene
- Child pornography
- Harmful to minors

NOTE

A *visual depiction* is any picture, image, or graphic image.

FYI

E-Rate funding provides discounts to schools and libraries for Internet access and telecommunications services. This funding is collected as part of the universal services fee paid by consumers to use telecommunications services. The goal of this funding is to help all schools and libraries have affordable Internet access. Discounts range from 20 percent to 90 percent of the service costs depending on the need of the school or library. Part of the E-Rate application requires schools and libraries to state affirmatively that they are complying with CIPA.

Under CIPA, *obscene* and *child pornography* are defined by referring to other laws. CIPA does specifically define the phrase *harmful to minors*. It includes any visual content that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors[17]

Scope of the Regulation

Any school or library that receives federal funding from the E-Rate program must comply with CIPA. The E-Rate program provides discounts to most schools and libraries for Internet access. Schools and libraries don't have to accept these funds. They can either pay for the Internet access with other funds, or choose not to use the Internet.

Main Requirements

CIPA has two main requirements. The first is that schools and libraries that accept E-Rate funding must implement technologies that filter offensive visual content so that minors don't access it. The second requirement is that schools implement an Internet safety policy.

Content Filtering

The primary requirements of CIPA mandate the filtering of content. Offensive content must be filtered so that minors don't see it. Although this may seem difficult, there are tools to make the job easier. CIPA's terms for such a tool is **technology protection measure (TPM)**. A TPM is any technology that can block or filter the objectionable content.[18] Remember that under CIPA, a TPM must filter visual content.

Consider Figure 5-1. This figure shows a proxy server used to filter content. A **proxy server** accepts Internet requests from clients, retrieves the pages, and serves them to the client. Content filters filter out objectionable content. As shown, you'd configure the internal clients to access the Internet through a proxy server.

The proxy server has a content filter. This content filter blocks all content marked as unacceptable. Some filters can also block content to e-mail and instant messaging programs. Similarly, the filter allows all content marked as acceptable. The proxy server identifies what's acceptable based on filter lists.

Third-party companies sell subscriptions to filter lists. These companies constantly search the Internet. They identify restricted materials and add it to the filter lists. When a network administrator adds the filter to an organization's proxy server, the server blocks the prohibited material.

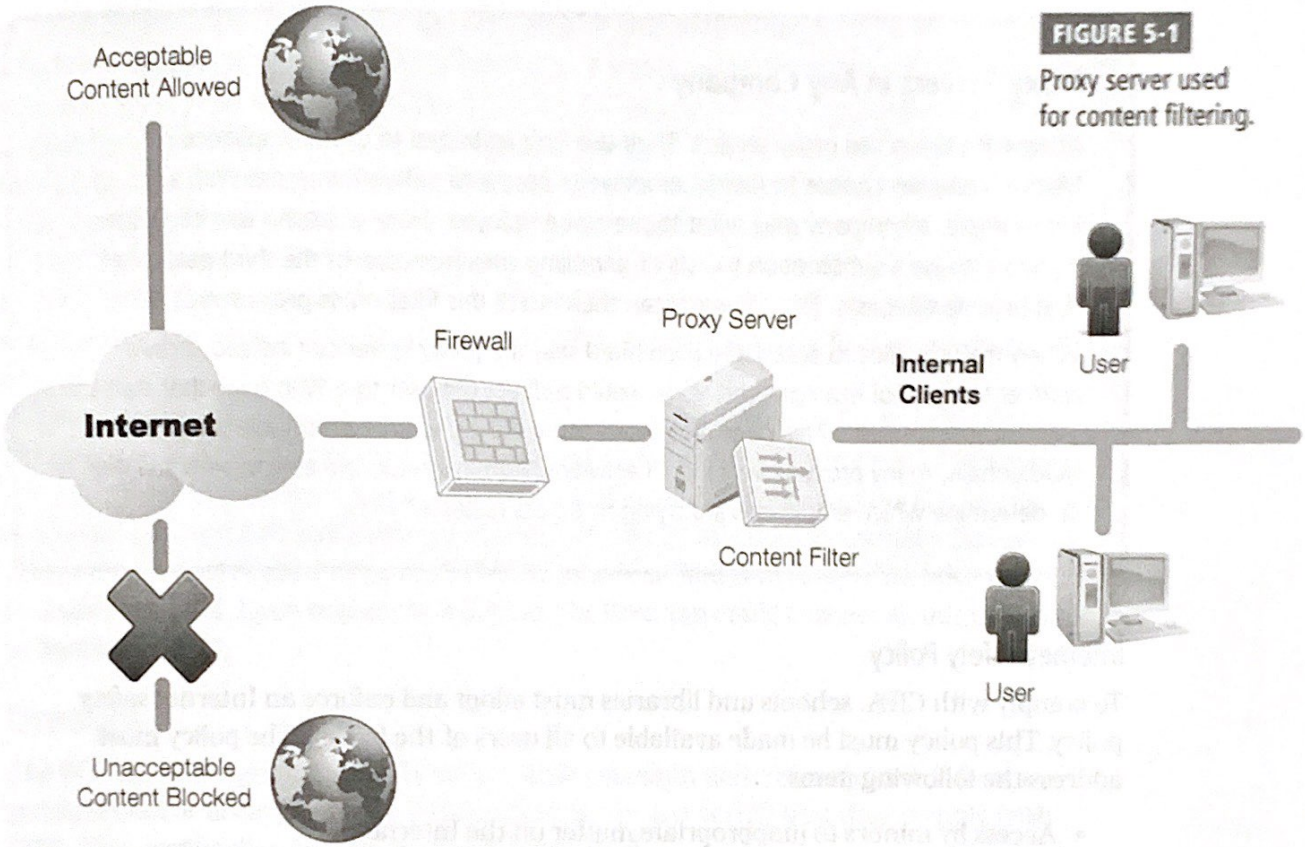

FIGURE 5-1
Proxy server used for content filtering.

In addition to filtering with lists like the ones described above, TPMs can also include monitoring technologies that track a child's online activities. They can also limit the amount of time that a child can spend on the Internet. TPMs also include age-verification systems that restrict online access to adults.

The Federal Communications Commission (FCC) recognizes that a TPM cannot be 100 percent effective.[19] However, neither CIPA nor the FCC defines what level is acceptable. A third-party company may claim its filter is CIPA compliant. However, there is no certification process to verify that a filter is CIPA compliant. The FCC has stated that local authorities should determine which measures are most effective for their community. The FCC rules specifically state that the U.S. federal government may not establish the criteria for making this determination and that it must be handled at the local level.[20]

Although a proxy server is a common method of filtering, CIPA doesn't specify where to filter the content. An Internet service provider (ISP) may be able to filter it. You may be able to purchase software to install on individual computers for filtering purposes. CIPA states what must be filtered but not how to filter it.

Proxy Servers in Any Company

Many companies use proxy servers. Their use isn't restricted to CIPA compliance. Many companies choose to restrict employee's access to different Internet Web sites. For example, a company may want to prevent employees from accessing gambling sites. It can purchase a subscription to lists of gambling sites from one of the third-party sites that provide filter lists. The company can then install this filter on its proxy server.

When the user tries to access the prohibited site, the proxy server can instead show a different page. For example, the server could redirect the user to a Web page that states, "Access is restricted." This page also could show the company's acceptable usage policy. Additionally, many proxy servers log all activities. Administrators are able to view the logs to determine which employees are trying to access restricted sites.

Internet Safety Policy

To comply with CIPA, schools and libraries must adopt and enforce an Internet safety policy. This policy must be made available to all users of the facility. The policy must address the following items:

- Access by minors to inappropriate matter on the Internet
- The safety and security of minors when using electronic mail, chatrooms, and other forms of direct electronic communication
- Unauthorized access, such as "hacking," and other unlawful activities
- Unauthorized disclosure, use, and dissemination of a minor's personal information
- The measures designed to restrict minors' access to harmful materials

An Internet safety policy must educate minors about appropriate online behavior. This includes how to use social networking Web sites and chatrooms safely. The policy must include information on how to recognize cyberbullying. It also must tell minors how to respond to cyberbullying.[21]

Exceptions

One of the main criticisms of CIPA is that schools and libraries are not implementing it properly. CIPA requires schools and libraries to filter visual depictions that may be harmful to minors. This means that images must be censored. However, sometimes access to text and entire Web sites are blocked. In addition, sometimes the TPMs used by libraries may not work correctly and may actually allow minors access to obscene materials. Finally, often TPMs deny access by both adults and children to constitutionally protected content.

According to CIPA, a school or library must be able to disable the TPM for any adult who has a need to view content for a research or other lawful purpose. An adult is anyone over the age of 17. If a school or library refuses to disable a TPM for an adult that requests it, then the school or library is potentially infringing on the First Amendment rights of that adult. This is because they are censoring adult access to protected content. Under CIPA, an adult doesn't have to state why he or she wants the TPM disabled.

The *United States et al. v. American Library Association, Inc. et al.* Supreme Court ruling in 2003 explicitly mentioned this point. One of the reasons that the Supreme Court held that the law was constitutional is because a TPM could be disabled for any adult that requests it.

Libraries can use any method to disable the TPM that works best for their location. For example, library personnel could label some computers as "adult only." Librarians would then have to monitor and prevent minors from using these computers. Librarians also could log onto a program designed to disable the TPM. Only personnel with the proper credentials could disable the TPM. Another method is to require an administrator to disable the TPM. Upon request by a patron, the librarian could contact an administrator to disable the TPM.

Oversight

The FCC has oversight for CIPA. However, little oversight action is required. When a public school or library requests E-Rate funding, it must certify that they comply with CIPA. This certification is usually all that is required.

If a TPM fails, the school or library is expected to take steps to resolve the failure. Patrons may complain to the library for specific instances such as a TPM blocking too much content or not enough content. If the library doesn't resolve patron complaints, then the patron can file a complaint with the FCC. The FCC may investigate those complaints. Any school or library that fails to comply with CIPA must refund any E-rate funds or discounts that it received. Depending on the situation, other criminal laws such as laws against providing false statements to the government could apply to CIPA violations.

Family Educational Rights and Privacy (FERPA)

The Family Educational Rights and Privacy Act (FERPA) passed in 1974.[22] The primary goal of FERPA is to protect the privacy of student educational records. An *educational record* includes any personal and education data on a student maintained by an educational agency or institution. Under FERPA, parents have the right to inspect and review a student's educational records. These rights do not belong to a parent forever. When the student reaches age 18, these rights pass to the student.

Scope

FERPA applies to any education agencies or institutions that receive funding from the U.S. Department of Education (ED). Educational agencies or institutions include:

- Primary and secondary schools
- Vocational colleges
- Colleges and universities
- Community colleges
- State and local educational agencies
- Schools or agencies offering preschool programs

For readability, the phrase "educational agency or institution" will often be shortened to "school" in this section.

The type of funding that these institutions receive from the federal government can be direct or indirect. Schools may receive funding outright from the ED. This is direct funding. If a college student receives a federal grant or federal aid and uses this as payment to a university, then the university is receiving federal funding. This is indirect funding and the university must comply with FERPA. Because federal funding is so valuable, and comes from so many different sources, almost all schools comply with FERPA.

If any educational agency or institution chooses not to comply with FERPA, it can't receive any federal funds. Sometimes private schools and universities don't receive federal funds. In these cases, these institutions don't have to comply with FERPA.

NOTE

FERPA formally defines personally identifiable information (PII). Several other laws and regulations also define PII. PII can be a name, a Social Security number, biometric data, or any data used to identify a person. Several laws and regulations specify different types of PII that must be protected.

FERPA and Peer-Grading

Many professors use peer-grading techniques. Students may be required to work in a project together and grade each other at the completion of the project. Additionally, students may be required to exchange assignments or tests and grade each other. Some professors require students to call out other students' grades in class. This is acceptable under FERPA.

Under FERPA, a school can't publish students' grades. This includes publishing grades on a bulletin board outside of a classroom. This prohibition doesn't extend to peer grading. The U.S. Supreme Court decided this in 2002. In *Owasso Independent School District No. I-011 v. Falvo*, the court decided that peer grades are not maintained as education records. FERPA does not protect them from disclosure.

Main Requirements

FERPA has four main requirements: Annual notification, access to education records, amendment of education records, and disclosure of education records.

To carry out these requirements FERPA has several important definitions.[23] These include:

- **Student**—Any individual that has ever been in attendance at an educational institution and for whom the institution maintains education records.
- **Attendance**—A student's physical attendance at an educational institution. It includes any virtual attendance such as video conference or correspondence course. Attendance via the Internet, by satellite, or through other methods used by the school is also included.
- **Education records**—Any records related to a student maintained by an educational agency or institution. These include written documents, computer media, video, film, or photographs. Records maintained by any outside party acting for the agency or institution are also included.

FERPA also defines personally identifiable information (PII) and places limits on how this data can be used and disclosed. Under FERPA, PII includes:

- A student's name
- The name of the student's parent or other family members
- The address of the student or student's family
- A personal identifier, such as the student's Social Security number, student number, or biometric record
- Other identifiers, such as the student's date of birth, place of birth, and mother's maiden name
- Other information that is connected to a specific student that would allow a reasonable person in the school community to identify the student
- Information requested by a person who the school reasonably believes knows the identity of the student to whom the education record relates

It's important to know what might be included in a student's education record. The rules can be complex. Demographic information such as race and gender can't be given out if it's directly connected with a student name. FERPA protects grades or transcripts of grades. Disciplinary records are considered a part of the student educational record. Behavioral notes on the student are also protected if the notes are kept in the student record. Under FERPA the private notes of faculty and staff are not usually considered educational records. If the faculty or staff notes are kept in a student record then they're considered part of the educational record.

It's possible for a student record to contain additional information outside the scope of FERPA. FERPA doesn't require schools to reveal this data when access to an educational record is requested. For example, a school doesn't have to reveal parental financial records, confidential letters of recommendation, or statements of recommendation.

NOTE

Eligible students are students over the age of 18. FERPA parental rights transfer to the student when the student turns age 18.

Annual Notification

FERPA requires schools to provide an annual notification to students and parents. This notice lets parents and eligible students know what their FERPA rights are. The annual notification also must state how to file a complaint with the Department of Education if the school violates any of FERPA's provisions.[24]

The annual notification must identify school officials that have access to educational records without consent. FERPA allows any school official that has legitimate educational interest in the record to view it without specific consent. These officials must be identified in the annual notification. The school has great freedom in identifying these officials. They could be teachers, instructors, professors, administrative personnel such as principals or provosts, or local board of education personnel.

Finally, FERPA requires that the school provide the annual notice "by any means that are reasonably likely to inform the parents or eligible students of their rights."[25] This means that the school might have to translate the notice into different languages. It also must consider whether it should provide the notice in alternative formats to disabled students or parents.

Access to Education Records

The most fundamental right under FERPA is student and parental access to the student's educational records. The parent or eligible student has the right to inspect and review any educational records maintained by the school.[26] Under FERPA, schools must respond within 45 days to a request to inspect and review educational records.

In most instances, the school doesn't have to make copies of the records. It only needs to make them available for review and inspection. If the parent or student requests copies, the school may charge a small copying fee.

There are special access rules for colleges and universities. These rules apply to situations where an educational record for the student may also contain confidential information about the student's parents. This happens often in situations where parents provide their own financial information to help a student receive federal financial aid. In these situations, colleges and universities don't have to give a student access to the financial records of his or her parents.[27]

FYI

Schools are required to make and provide copies of the educational records in special circumstances. If a parent does not live within commuting distance to the school and cannot come to the school to inspect the records, then the school must provide the parent with copies.

Finally, a school is not required to create an educational record where none exists. Sometimes students or parents might request a report or record that is not already part of the educational record. In these cases, the school doesn't have to create that report just because a parent asked for it.

Amendment of Education Records

FERPA allows parents and students the right to request amendment of student educational records. A parent may ask that a school amend information in the record that is incorrect or misleading. The school's annual notification must specify the procedure for how to request this correction.[28]

Schools are not required to honor the request for correction if the school doesn't believe that the student's record is incorrect. The school must notify the parent or student of this decision. If a school doesn't amend a student educational record, then the parent or eligible student has the right to a hearing on that decision.[29] The purpose of the hearing is to determine if the schools decision was appropriate. The school and the parents will present their cases to the hearing officer. If the hearing officer decides that the school's decision was appropriate, then the parent or eligible student must be allowed an opportunity to provide a written statement that's added to the student's educational record. The written statement can comment on the information under dispute in the record. It can also state why the parent or student disagrees with the decision of the school not to amend the record.

> **NOTE**
>
> Schools are required to hold hearings on amendment disputes within a reasonable time after it receives a request for a hearing. The school must give the parent or eligible student notice of the time, date, and location of the hearing.

Disclosure of Education Records

In general, educational agencies or institutions must have permission from either a student or the student's parents in order to disclose educational records and student PII. The school must obtain written consent to release this data. Most schools have forms for this purpose. The procedure for using these forms is usually included in the school's annual notification.

To disclose student educational records, written consent must include:

- Which records will be disclosed
- The purpose of the disclosure
- Who will receive the record
- The date the consent is granted
- Signature of the student or parent
- Signature of the school official releasing the data[30]

Parents and students can refuse to give consent to have their data released. The school can still release data to certain entities. The next section explains these exceptions.

> **NOTE**
>
> It's important to remember that the parent has these rights until the student reaches the age of 18. After that point, the parent no longer has the rights. Only the child has the rights. In other words, a parent may be paying for a 20-year-old son or daughter's college education, but the parent doesn't have the right to inspect their child's educational records.

Disclosure Exceptions

A school can release student records without prior consent in some cases. As mentioned earlier in this section, school officials, such as principals or teachers, can view student educational records. These officials must have a legitimate educational interest to view the record. School officials can't view a student record merely if they are curious about a student's performance.

Directory information can also be released without student or parental consent. Directory information includes a student's name, address, telephone number, date and place of birth, awards, and dates of attendance. Under no circumstances should the directory information include PII information such as a student's Social Security number or student identification number.

Schools must identify which student data is specifically defined as directory information. Schools also must tell parents and eligible students how to request that the school not share this information. All of this information must be included in the school's annual notice.[31] The release of directory information is the primary FERPA disclosure exception. Schools frequently rely on this exception.

FERPA allows a school to disclose student PII in a number of other ways that don't require prior written consent:

- Schools can transfer a student's educational record to a new school if a student is moving from one school to another.
- Schools can provide student PII to an accrediting organization to prove that the school is performing to specific standards.
- Schools can provide student PII in some financial aid situations.
- Schools may disclose student educational records in response to a court order or lawful subpoena.
- School may disclose student PII if it will aid personnel in an emergency situation.
- Post-secondary schools can disclose the PII of a student over age 18 to that student's parents if the student is considered a dependent for U.S. federal tax purposes.

Schools must maintain records of all of the requests and disclosures of student educational records.[32] These records must include the parties who received the student PII and the reason for the disclosure. This record of disclosures must be maintained for as long as the school maintains the underlying educational record.

Security of Student Records Under FERPA

FERPA has no specific information security requirements that schools must use to protect student educational records. For example, FERPA does not contain a requirement that schools notify parents and students if an unauthorized person accesses student records. Instead, schools just have to record the unauthorized disclosure in the student record.

How to Respond to Requests

A school may receive many different kinds of requests for information. Any personnel that have access to records should have training on how to respond. Put yourself in the situation of the person answering the phone. How would you respond?

An employer calls and asks about a student who graduated last year. Specifically, the employer asks if the student graduated. Does FERPA restrict the release of this information? How do you respond?

- FERPA covers this information. You may need to explain this to the employer.
- You can give the information to the employer if the student signs a consent form.

A student needs a copy of his transcript. He asks a friend to pick it up for him. What should you tell the friend when he shows up?

- FERPA restricts the school from giving the friend this information.
- You may check the student's record to see if it has a signed consent form for this friend. If not, the transcript shouldn't be given out.
- The student must sign a consent form.

A mother calls about her 18-year-old son. She wants to know if her son will be graduating with his class. Does the parent have rights to this information? What do you tell her?

- FERPA rights transferred to the son when he turned 18. The parent doesn't have rights to this information. You may want to explain the FERPA requirements to the mother.
- Encourage the mother to talk with her son. In other words, ask her son if he will be graduating. You can provide information on how someone can reenroll in classes.

The mayor recently made a speech and mentioned a student at your school. The mayor talked about how the student had earned a specific degree and was now working on a higher-level degree. You know that the student never completed any degree at your school. What should you do?

- FERPA protects this information. You shouldn't take any action.
- If the mayor or the mayor's office requests the information, you can't release it without a consent form.

Even though it is not required under FERPA, the U.S. Department of Education does encourage educational institutions to take steps to protect student information. The department suggests that schools consider the following factors to implement security measures:

- The type of information to be protected
- The size and complexity of the educational institution
- The resources available to the institution
- Security safeguards used by other institutions in similar circumstances[33]

Oversight

The Family Policy Compliance Office (FPCO) in the U.S. Department of Education provides oversight for FERPA. This office investigates FERPA complaints. Only parents and students over the age of 18 may make complaints against schools for FERPA violations. Complaints must be submitted to the FPCO within 180 days of the date that the FERPA violation is alleged to have occurred.[34] The FPCO resolves FERPA complaints and enforces its decisions by withholding federal funding to the school that have violated the law.

Case Studies and Examples

The following case studies provide some real-world background on COPPA and FERPA. These examples provide insight into how the laws are challenged and viewed.

Liberty Financial and Children's Privacy

In 1999, the FTC charged Liberty Financial Companies, Inc. (Liberty Financial) with making false promises. These false promises were related to the collection of personal information from children and teens. In this complaint, children were identified as anyone under 13. Teens were identified as anyone aged 13 to 17.

Liberty Financial hosted a Web site at younginvestor.com. It targeted children using contests and prizes. At one point, Liberty Financial created a survey called The Young Investor Measure Up. The survey's introduction stated, "All of your answers will be totally anonymous." The survey then collected information such as:

- Amount of allowance
- Gifts of stocks, bonds, or cash
- Spending habits
- Part-time work
- Plans for college
- Family finances

The survey ended with a request for name, address, and e-mail. It stated this information would be used to send a newsletter and award a prize every three months. Clearly, this information removed the child's anonymity. Additionally, Liberty Financial didn't send any newsletters. Neither did they award any prizes.

Liberty Financial was required to post a clear and prominent privacy policy on its Web sites directed to children under 13. The FTC also required Liberty Financial to obtain verifiable parental consent before collecting or using information for children under 13. These requirements were directly related to compliance with COPPA. The case occurred between the time when COPPA was passed and when compliance was required 18 months later.

The FTC documents related to the Liberty Financial case are available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/1999/08/liberty-financial-companies-inc.*

Iconix Brand Group, Inc.

In *United States of America v. Iconix Brand Group, Inc.*, the FTC alleged that the site falsely represented that personal information would be maintained anonymously. Instead, the data was collected and maintained in such a way that children could be identified.

In 2006, the FTC charged Iconix Brand Group, Inc. (Iconix) with failing to comply with COPPA and for engaging in deceptive tactics. Specifically, the FTC charged that Iconix was deliberately collecting information on children. However, the Iconix Web site's privacy policy specifically stated it was not. Part of the privacy policy stated:

> We do not seek to collect personally identifiable information from persons under the age of 13 without prior verifiable parental consent. If we become aware that we have inadvertently received such information online from a child under the age of 13, we will delete it from our records.

Although the policy was sound, the company didn't follow it. The Iconix Web sites clearly targeted children. Iconix had domain names such as MuddGirls.com and Candies.com. Web site graphics included cartoon characters and photos of young girls. Over 1,000 girls under the age of 13 allegedly registered on Iconix Web sites between 2006 and 2009. This was determined based on birthdates given by the registrants.

The FTC concluded that the Iconix sites were targeted for children. The FTC based the conclusion on the activity of the Web site, not just the privacy policy. Further, the FTC concluded that Iconix was deliberately trying to avoid the requirements of COPPA. Iconix ultimately paid a fine of $250,000 to settle the case.

The FTC documents related to the Iconix Brand Group case are available at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2009/10/united-states-federal-trade-commission-plaintiff-v.*

Gonzaga University Student

Gonzaga Univ. v. Doe involves a graduate who was denied the ability to become a public school teacher because of information released by the school. The student sued and won. Monetary damages were awarded to the student. However, the U.S. Supreme Court overturned the case stating that the student can't sue the university for damages based on violating FERPA.

FYI

Gonzaga Univ. v. Doe doesn't address whether the school did the right thing related to FERPA. Instead, the focus is on the ability of the student to sue a school for a violation of FERPA. This is known as a *private cause of action*. The Washington State Supreme Court agreed that the student could sue. The U.S. Supreme Court overturned this and stated that FERPA doesn't create any individual rights that can be enforced.

The student graduated Gonzaga University in Washington State and planned to become a public elementary school teacher. The student needed to provide an affidavit of good moral character from her college. The teacher certification specialist at Gonzaga University contacted the state certification agency and provided damaging information. This specialist indicated that the student was engaged in sexual misconduct and identified the student by name. The student didn't receive the affidavit from the school and didn't get the job.

A jury ultimately awarded the student compensatory and punitive damages. The school contested this to the Washington State Supreme Court. The state supreme court upheld the verdict. However, the U.S. Supreme Court reversed the decision. In a 7–2 decision, the U.S. Supreme Court said that FERPA does not give the student personal rights that can be enforced. In other words, the U.S. Department of Education could bring a lawsuit against the school. However, the student doesn't have the right to sue.

Documents related to the Gonzaga University case are available at *http://www.law.cornell.edu/supct/html/01-679.ZS.html*.

Release of Disciplinary Records

Disciplinary records are a part of student records. FERPA protects student records, which include disciplinary records. A student's consent is required prior to releasing any of these records.

A U.S. district court in the Southern District of Ohio decided this in 2000. The U.S. Court of Appeals affirmed the decision in 2002. However, the case actually started in 1995 and has a colorful history.

In 1995, the Miami University student newspaper asked Miami University to provide disciplinary records on students. This was to track crime trends on campus. The university refused to release the records. The paper then made a request using the Ohio Public Records Act. Miami University released the records but removed all personally identifiable information. They also removed information such as the date, time, and location of the incidents.

Editors of the paper thought that the university removed too much information from the records. They went to the Ohio Supreme Court seeking full disclosure of the records. In a divided decision, the Ohio Supreme Court agreed and ruled that FERPA doesn't cover the disciplinary records. Miami University tried to take the case to the U.S. Supreme Court, but the court chose not to hear the case in 1997.

Miami University notified the U.S. Department of Education (ED) that it didn't think it was able to comply with FERPA based on the decision. The university also adopted a policy of releasing disciplinary records to any third-party requestor. Ohio State University also released records and notified ED that it planned to honor future requests. ED disagreed and thought that the Ohio Supreme Court made a mistake.

ED filed a motion to stop both universities from releasing these records. The U.S. district in the Southern District of Ohio heard the case. The universities didn't dispute the facts and were willing to allow the court to rule. However, the school newspaper filed a motion to intervene. Although the newspaper wasn't named in the suit, it wanted its voice heard.

The newspaper claimed that ED didn't have authority in the case. Instead, ED could take action only after the release of records, not before. However, the circuit court disagreed. It determined that ED did have authority. Additionally, the circuit court determined that disciplinary records are education records and covered by FERPA. The court ordered the universities not to release the information.

The newspaper appealed this decision to the U.S. Court of Appeals. The newspaper argued that FERPA violates the First Amendment and the district court didn't recognize this violation. However, the U.S. Court of Appeals upheld the district court's decision in 2002. Even today, schools must not release student disciplinary records without student consent.

ED documents related to the Miami University case are available at *http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/unofmiami.html and http://www2.ed.gov/policy/gen/guid/fpco/courtcases/miami.html*.

CHAPTER SUMMARY

This chapter covered several laws designed to protect the rights of children and students. The Children's Online Privacy Protection Act (COPPA) protects the information of children. It prohibits Web sites from collecting information about children without a parent's consent. COPPA defines a child as anyone under the age of 13.

The Children's Internet Protection Act (CIPA) requires schools and libraries to filter Web site traffic. CIPA ensures that children don't view objectionable material from these publicly funded locations. CIPA defines a child as anyone under the age of 17.

The Family Educational Rights and Privacy Act (FERPA) requires schools to protect educational records. Schools need written consent prior to releasing educational records. The student or parent has the right to review these records. FERPA grants these rights to the parent until the child reaches the age of 18. At that point, the right passes to the student.

KEY CONCEPTS AND TERMS

Parental controls
Proxy server
Technology protection measure (TPM)