



Curriculum Units by Fellows of the Yale-New Haven Teachers Institute
2000 Volume III: Constitutional and Statutory Privacy Protections in the 21st Century

Constitutional Privacy in the 21st Century The Information Highway & Your Right to Privacy

Curriculum Unit 00.03.03
by Leslie Judd-Paier

The curriculum presented in this unit is to be used in a business law class next year and the years to come. We will study the United States Constitution and Bill of Rights, with a major focus on the 1st and 4th Amendments and how they relate to the Internet and constitutional privacy in the 21st century.

In the twenty-first century we find ourselves surrounded by a world of mass communication, high technology and instantaneous transmissions of words and visions. People all over the globe can communicate by telephone, by computer and by facsimile machine in seconds. We can talk, we can write, and we can send pictures. This ability to communicate via the Internet has enhanced the lives of people around the globe in many ways. It has also raised new legal and ethical questions.

In particular this unit addresses issues regarding the 1st and 4th Amendment rights of American citizens. The 1st Amendment focuses on your right of free speech while the 4th Amendment deals with your right to privacy. However, both these Amendments are limited to the powers of the federal government. They do not protect citizens from other private individuals or businesses.

The 21st century promises to bring even more technological advancement than the 20th century. Already, the Internet has expanded far greater than ever imagined. If you compare the growth of the Internet to the Industrial Revolution it has grown exponentially times faster. One of the problems faced during the Industrial Revolution was the governments ability to create laws fast enough to protect citizens. Many share this same concern with regard to the Internet.

Leaders of the Industrial Revolution, like Rockefeller, Carnegie and J. P. Morgan, just to name a few, took the country by surprise. They created a new world in which the ways society functioned and business was conducted was changed forever. New laws were enacted which changed the way business is done. Laws that made business monopolies illegal were created. Other laws to protect American citizens from corporate malfeasance were created as well.

We are now experiencing a problem with the Internet similar to that of the Industrial Revolution. The legal system, businesses, Internet users and members of society must now look and ask themselves the following questions:

Are laws being made and passed to protect users on the Internet?
How long will it take for laws to be made to protect citizens?
Who will the laws protect? Honest citizens, sleazy citizens, all citizens or just big business?
How will all the parties be protected?
Will the laws protect people's privacy, while permitting legitimate business on the Internet?

Audience

Business law is taught to high school students in grades 10 - 12. The school setting is in an urban community. Students attending the class are of varying ability levels, ranging from straight "A" students, to students who have difficulty reading and writing. Business law is an elective.

Purpose

The purpose of this paper is to enhance classroom lesson plans with new, interesting and pertinent information which students can relate to and use in their daily lives.

THE STUDENT WILL LEARN ABOUT:

The United States Constitution and the framework it provides to our federal government
The 1st Amendment and the protection it provides citizens, with an emphasis on free speech and how it relates to the Internet
The 4th Amendment and the protection it provides to individuals and their right to privacy and how that relates to the Internet
The creation of statutory and case law relating to the Internet.

The Internet will be used as our primary subject of discussion.

Upon completion of this unit, students will have a better understanding of how they are protected by the 1st and 4th Amendments in the Bill of Rights. They will gain an understanding that there are responsibilities that accompany the freedoms we enjoy.

Teaching Strategies and Rationale

The students will gain a better understanding about their rights to privacy and freedom of speech via the Internet by learning about their 1st and 4th Amendment rights. Studying various source materials will help the students do this. Lessons are designed to capture student interest through relevant issues facing society today. Lessons begin with thought-provoking questions and include hands-on activities.

It will be necessary for teachers and students to keep up with current issues through web sites, newspaper reports and magazine articles, just to name a few. Classroom discussion will definitely capture and entertain student interest. Teachers should try to keep the students focused on only the 1st and 4th Amendment issues. There are many other constitutional issues, but try to keep students from digressions.

Lesson plan 1 discusses computer crimes. This will open the door to a great amount of discussion. Have students come up with a list of crimes they can think of off the top of their heads. Teachers should add to the list if it is not complete. Next, discuss with students laws which they believe should be made to protect their privacy. Ask students how these laws might affect their 1st and 4th Amendment rights. Ask students to list the positive and negative aspects each law might have on citizens. Ask students who in particular benefits from the laws they have listed. Is it the private citizen or big business? Ask students what they think will be the monetary effect if such laws are created? Ask students if certain laws are made to protect their privacy, should citizens be concerned about the monetary effect it might have on their pocketbooks? The lesson activity has students doing hands on research at the Department of Justice Cybercrime web sites.

Lesson plan 2 brings out the issue of anonymous speech. The case of *Aquacool_2000 v. Yahoo* will be read. I believe students will be interested in anonymous speech, and a real and current court case will spark their interest. Students will benefit because they can learn about anonymous speech and see our legal system at work.

Lesson plan 3 gives students hands-on Internet research. Students will learn about privacy issues first hand from Internet users and privacy advocate groups. I believe this will open up to students additional issues which they might not have thought of themselves.

In lesson plans four and five, students are asked to write letters to their congressperson. Teachers should write their congressperson ahead of time and request that a reply is sent to students. This will add meaning to the lesson and show students that their representative is listening to them.

What is the Internet?

The Internet, often referred to as the NET, is a general purpose, international communication and information system. Once you have access to the Net, there are many things you can do. You can send and receive messages, access a great deal of information, and participate in ongoing discussions with people all over the world. You can also play games, look at pictures, listen to music, watch videos, chat with people, go shopping, and find lots of free programs for your computer. The Internet is a complex collection of resources (Harley Hahn Teaches the Internet, 1998 p. 2)

The Internet was originated in the late 1960s by the federal government's Pentagon Advanced Research

Projects Agency (ARPA). This group began developing an experimental computer network aimed at withstanding a military attack. The Internet provided a medium for communications between universities, researchers and the government.

Within the past ten years, the Internet has grown exponentially. It has changed the way people communicate and the way many businesses do business. The Internet gave birth to e-commerce and opened the commercial world to small and home based businesses. The Internet has made what we thought of as an already efficient world even more efficient, at least in some ways.

I compare the explosion of the Internet to the “Wild West,” a time when people made their own laws. Today, as the Internet continues to develop, there are very few laws regarding this new phenomenon. In a way, the Internet and society as a whole are in the same type of exploratory environment as the “Wild West” once was.

The legal terrain of the Internet and its boundaries are still being defined and tested. New boundaries are being explored and the limits are unknown. Because the Internet is so new and its widespread use was not as anticipated, laws to protect a person’s privacy are not in place. Innumerable legal controversies relating to the Internet are beginning to surface.

For example, the expansive reach of the Internet has spurred a new debate over the individual’s right to privacy. The debate surrounds our right to choose whether personal information collected over the Internet can be disclosed. The debate also concerns our right to know how, when, and how much of our personal information is being collected, who is collecting it, and how it is being used.

An Electronic Bill of Rights for this electronic age is a key government initiative. The Electronic Privacy Information Center has called for legislation to enact privacy policies for the Internet. Several pending bills (E-Privacy Act, Data Privacy Act, and Consumer Internet Privacy Act) would regulate Internet activity in the name of privacy (Law for Business and Personal Use, 2000 p. 40).

US Constitution and Bill of Rights What makes the United States Constitution the most influential document of its kind in the history of the world?

- The U.S. Constitution created the United States of America

- The U.S. Constitution included a Bill of Rights

- The U.S. Constitution is a working document

- The U.S. Constitution created a system of checks and balances

When the United States Constitution was written in the late 1780’s, our founding fathers (and perhaps mothers) feared that future violations of our fundamental rights by a strong central government would still be possible. The citizens of our new country-to-be felt the document was incomplete. They would not vote for the Constitution until they were guaranteed a certain “Bill of Rights”.

The Bill of Rights, the common name for the first 10 amendments, completed the Constitutional framework

that provided protection from possible intrusion from the federal government. The U.S. Constitution with the Bill of Rights has been our legal guide and protector from the abuses of power and government.

Fortunately, the fifty-five delegates who drafted the U.S. Constitution wrote it as a living and working document, allowing for changes to be made as necessary. The founding fathers had great foresight in doing so. The U.S. Constitution provided the legislative branch of our government and the people the power to amend our constitution when necessary.

The U.S. Constitution created a system of checks and balances. This means that equal authority is given to the three basic branches of government: the judicial, the executive and the legislative. Warren E. Burger, former Chief Justice of the U.S. Supreme Court, pointed out that, “there was no country in the world that governed with separated and divided powers providing checks and balances on the exercise of authority by those who governed” (Law for Business, 1993 p. 6,7)

By studying the Communications Decency Act (1996), students will see how the system of checks and balances is put to work to protect and uphold the Constitution and individual rights. The CDA 1996, which was passed by our legislative branch, was found unconstitutional in 1997 by our judicial branch.

The U.S. Constitution and the Internet are still trying to find their place together. The Internet is a land without boundaries. The Internet at times is an institution without regard for law. The U.S. Constitution is a framework which must be preserved to provide continuing structure to protect its people. The Internet is a society which still needs to be tamed. The questions are to what degree and how.

The 1st Amendment - Focus on Free Speech and Your Right to Privacy

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”

As a country, we pride ourselves on the existence of the United States Constitution and Bill of Rights. We are especially proud of our 1st Amendment right, the freedom to express ourselves and to speak freely. We are free to say what we think even in the face of controversy. We are especially free to criticize the government. Our job as citizens is to make sure that we are responsible in what we say when we exercise our 1st Amendment rights.

The Internet is a collection of information on any subject. The Internet is a global network of computers. This network can connect with anyone, any web site, any time. You can make your voice, pictures and thoughts heard via the Internet to any interested party. The 1st Amendment stands to protect these Internet voices.

Our government has tried to censor web sites on the Internet which show inappropriate material. The government says that one major problem with free speech and expression on the Internet is that a minor can easily gain access to sexually explicit web sites. For example, if you are looking for the official U. S. White House web site on the Internet and you type in <http://www.whitehouse.com> instead of <http://www.whitehouse.gov>, you enter a pornographic web site with material not appropriate for minors or modest people.

Censorship

Censorship involves policing the Internet. The censoring body may prohibit what they consider to be immoral or otherwise objectionable. Many feel that such censorship is an infringement upon their 1st Amendment free speech rights.

Congress passed the Communications Decency Act of 1996, designed to protect minors. This was their first attempt to censor or to put safeguards on Internet web sites. The American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) took the case to the United States Supreme Court. On June 26, 1997 the Supreme Court affirmed the lower courts decision that the CDA was unconstitutional. The Supreme Court ruled that the CDA infringed on a person's 1st Amendment right. The CDA applied to commercial web sites as well as any non-commercial speech on the Internet (i.e. chat rooms, e-mail). The Supreme Court struck down the CDA because the 1st Amendment protects American citizens and their right to free speech.

Congress acted quickly and introduced additional legislation. HR 3783, the Child Online Protection Act (COPA), imposes criminal penalties against any "commercial" web site that makes material that is "harmful to minors" available to anyone under 17 years of age. Many argue that this also is an infringement upon their constitutional 1st Amendment right. They claim the burden of censorship should be on the parents and not the government (www.epic.org/free_speech/copa/ 5/17/2000).

The ACLU and EPIC have now challenged COPA. U.S. District Judge Lowell A. Reed issued a temporary restraining order against the enforcement of COPA. Judge Reed noted that this case involves a "clash between 1st Amendment rights and the nation's responsibility to protect children."

Congress continues to introduce new legislation. Currently Senator John McCain has introduced bill S. 1619. This bill would require schools and libraries to use filtering Software. Senator Daniel Coat introduced bill S. 1482. This bill would criminalize material that is "harmful to minors" on the Internet. Newspapers and magazine articles will be a very useful source for students on current legislation and issues affecting Internet users and protecting their 1st Amendment rights.

Anonymous Speech

The Internet can also be a place where persons can hide their identities. You can communicate anonymously. The Internet users can actually become their pseudonyms. Individuals may stand up and voice their thoughts and opinions no matter how controversial they might be. Anonymity and pseudonyms are a way to protect privacy. Anonymous speech shields the person who wishes to remain a private party, but allows them to speak against what may be the majority. The following two cases are good examples of people practicing anonymous speech.

Aqualcool_2000 v. Yahoo! Inc. is a case currently being heard in court. Aquacool_2000 was participating in an online chat room. He was voicing his displeasure about a public company. The company subpoenaed Yahoo for the anonymous user's real name. Yahoo voluntarily gave the anonymous user's name without due process. This case considers many legal issues including Aquacool_2000's belief that his right to privacy has been

violated. For further details, review the case.

Under the 1st Amendment, the Supreme Court in *McIntyre v. Ohio Elections Commission*, 414 U.S. 334 (1995) ruled that anonymity “is not a pernicious fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.” The Court pointed out that the U.S. has a long tradition of protecting the right to communicate anonymously, beginning with the *Federalist Papers* in the late 1700s. This Supreme Court decision upheld the right to distribute anonymous political leaflets.

4th Amendment - Invasion of your Privacy and the Internet

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Americans say often enough, “I am entitled to my privacy.” But in fact privacy is a funny thing. No where in the U.S. Constitution is the word privacy used. The government of the United States has provided for our privacy without actually saying the word “privacy” in the Constitution. United States Supreme Court Justice Louis Brandeis explained a person’s right to privacy as “the right to be let alone.” As Americans, we believe our own personal business should remain just that, our own personal business.

When you begin to think about privacy, what information about yourself is actually private? You might find that there is more available information about you out “there” than you think.

Answer the following questions:

What personal information about yourself do you believe to be private?
What do you, a private citizen, do if your privacy has been violated?

What is privacy? Privacy is the right to keep some information about you secret. The Supreme Court states that we are entitled to a reasonable “expectation of privacy” (*Katz v. U. S.*, 389 U.S. 347,350 1967). What exactly does this mean? It may mean different things to different people. What is reasonable to one person may not be reasonable to another, based on their beliefs and life experiences.

Does everyone have an equal right to privacy? The answer to this question is, no. People who are considered “public figures” or newsmakers, including politicians, movie stars or just people who have made the news in some way, are not entitled to the same privacy as an ordinary citizen. In other words, they do not have the same reasonable “expectation to privacy.”

History of Privacy Law

Early invasions of privacy could be treated as trespass, assault, or eavesdropping. Part of the reason for the delay in recognizing privacy as a fundamental right is that most modern invasions of privacy involve new technology (e.g., telephone wiretaps, microphones and electronic amplifiers for eavesdropping, photographic and video cameras, computers for collecting/storing/finding information). Before the invention of such technology, one could be reasonably certain that conversations in private (e.g., in a person's home or office) could not be heard by other people. Before the invention of computer databases, one might invade a few persons' privacy by collecting personal information from interviews and commercial transactions, but the labor-intensive process of gathering such information made it impossible to harm large numbers of victims. Further, storing such information on paper in file cabinets made it difficult to use the information to harm victims, simply because of the disorganized collection of information (Standler, 1997 essay).

Privacy on the Internet?

We have become a society of convenience. We willfully give out personal information for the sake of convenience. While we are enjoying fast and efficient tasks, this convenience is costing individuals plenty when it comes to their privacy and the information they want to keep from others.

When we give this information to others, we have put the 3rd party in a position of trust. We must have faith in the system and believe that the credit card number you just gave out will only be used for your authorized purchase. We must have faith in the system and believe that your name, address, and Social Security number will only be used by the intended party and not by a person who will steal your identity and ruin your credit rating. At other times our faith leads us to cross our fingers and say a prayer.

As you navigate the Internet and different web sites, you may be asked for personal information. A web site might ask for your name, your e-mail address, your date of birth and your social security number. The web site may also ask for a credit card number. Under newly proposed legislation, this is supposed to be a way to confirm that you are not a minor.

Your mouse clicks are tracked on the Internet. When you click on a web site, your activity may be digitally archived. This archived data and activity tracking is known as a cookie. Cookies are used to track a person's identity, actions, and preferences as you explore the Internet. Many people are not familiar with cookies (Harley Hahn Teaches the Internet, 1998)

There is a big difference between knowingly giving out information about yourself and someone or something investigating who you are, what you do, and what you like. Are cookies and this type of tracking an invasion of privacy? I believe so.

What happens to the information cookies store? There are data aggregating companies who store this information about you. They may sell the information to a marketing company. This marketing company may in turn use this information about you and your preferences to market their products to you directly. Someone somewhere is storing information about you, the personal and private you.

This is a real issue and concern for all. If a company was to combine all your personal information such as your

preferences, your buying habits with your credit history, medical and educational information, they may put together a complete package of you. All this can be done, without you even knowing it. Does this make you feel comfortable?

Privacy in the Workplace

“EMPLOYEE BEWARE, YOU ARE BEING WATCHED.”

In Connecticut, the law states (Sec. 31-48d.) that employers may engage in electronic monitoring as long as they give prior notice to employees. The law defines “electronic monitoring” as the collection of information on an employer’s premises concerning employees’ activities or communications by any means other than direct observation. This may include the use of a computer, telephone, wire, radio, camera, electromagnetic, photo-electronic or photo-optical systems. The employer may not collect information (A) for security purposes in common areas of the employer’s premises, which are held out for use by the public, or (B) which is prohibited under state or federal law.

Employers who engage in any type of electronic monitoring must give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. The notice must be placed in a conspicuous place which is readily available for viewing by its employees.

Under the law, if an employer has reasonable grounds to believe that employees are engaged in conduct that violates the law, or the legal rights of the employer, or the employer’s other employees, or that creates a hostile work place environment, and (B) electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.

E-Mail

You probably view the E-mail you send as your own personal property. But what about the E-mail you send at work? Many companies now have E-mail policies about who owns the E-mail correspondence and whether the company considers the messages to be confidential. The courts have ruled that E-mails are the property of the company. In *Shoars v. Epson*, the judge found in favor of the company and stated that it had the right to tap into, read, and print employees’ E-mails. The court reasoned that the company’s property right in the computers prevailed. The company’s ethics was not of consequence, according to the current law. The bottom line: Be careful before you press the Send button. E-mail messages are neither confidential nor your private, exclusive property. (Law for Business and Personal Use, 2000 p. 288)

As a rule of thumb, employees should not use corporate e-mail accounts for their own personal communications. Employees should exercise a great amount of discretion when using E-mail. Most people forget and may say something that could be viewed by others as hostile or non-corporate friendly. This is what may get someone into trouble. When an employee uses corporate e-mail, they should be very careful as to what they write.

Ways to Protect Your Privacy on the Internet

Encryption is the ability to scramble data so an unauthorized party has a hard time listening in. Encryption software helps to preserve the sender's privacy. It gives the sender some reassurance that their freedom of speech and privacy (freedom from prying eyes) are protected.

Encryption software allows the user to transmit their data to another party. When the party on the receiving end opens the communications, they can decrypt the message. Prior to decryption, the message would be unreadable by most because it is in a scrambled form.

At one point, an executive order was issued by President Clinton limiting the exportation of encryption software for national security reasons. The governments thinking was that the use of encryption software would hamper law enforcement and intelligence-gathering abilities.

For a complete discussion and to gain a better understanding of why the government wanted to ban encryption software products look up <http://www.usdoj.gov/criminal/cybercrime/encryptfaq.htm>. This web site explains in detail law enforcement's point of view. For example, one question asked –

Isn't the government overstating the threat to our national security?

Their answer includes the following:

Not at all, law enforcement has already confronted encryption in high profile espionage, terrorist, and criminal cases. They cite the following examples:

1. An international terrorist was plotting to blow up 11 U.S. owned commercial airliners in the Far East. His laptop computer, which was seized during his arrest in Manila, contained encrypted files concerning this terrorist plot.
2. A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.
3. A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

They state that this is just the tip of the iceberg. Convicted spy Aldrich Ames, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to it.

The Internet community still believes the government's initiatives are infringements upon their 1st and 4th Amendment rights. They argue that the encryption restriction limits their free speech and ability to send communications over the Internet which would remain private.

Proposed Legislation

<http://rs9.loc.gov/cgi-bin/query/D?c106:32:./temp//~c106zHmzZ9::>

Online Privacy Protection Act of 2000 (Introduced in the House) HR 3560.

If passed, this law would require that the Federal Trade Commission protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet. This law would provide greater individual control over the collection and use of that information, and for other purposes.

1. The purpose of this law is to regulate a web sites unfair and deceptive acts and practices in connection with the collection, use and disclosure of personal information.

2. REGULATIONS

This bill would require the web site to:

- i) Provide notice on its web site in a clear and conspicuous manner, of the identity of the operator, what personal information is collected by the web site operator, how the operator uses such information, and what information may be shared with other companies; and
- ii) Provide meaningful and simple online process for individuals to consent to or limit the disclosure of personal information for purposes unrelated to those for which such information was obtained or described in the notice under clause i

This bill also requires the web site to:

- i) Provide a description of the specific types of personal information collected by the operator that was sold or transferred to an external company

Conclusion

The scope of the Internet, technology in the 21st century and your right to privacy is currently being shaped. This unit only begins to touch on the legal and ethical issues facing society and the legal community. Currently there are more questions than answers.

There are many issues and concerns: What will be the total cost of privacy for the American public? Will the costs be measured by losses of keeping personal information private? Will the costs be measured by the dollars spent by big business? Will the cost of privacy be driven by a society who wishes for convenience more

than for the protection of their privacy? Will an individual be able to voice their opinions and remain anonymous and uncensored?

At the present time your ability to keep information about yourself, what you do, and your preferences may no longer be possible. Your personal information is shared and sold by businesses and used on the Internet in many different ways. Privacy as we have come to know it and a reasonable expectation to it, seems to be waning.

Citizens must remember that just because a company or someone asks you for personal information, doesn't mean you have to give it. Some Internet users, when asked for personal information give the name Ima Nonymous. Many adults over the age of 50 have been only 35 years old for a long time. I don't encourage lying, but this might be a good rule of thumb to follow when companies ask for more information than they really need to know.

Recommendations have been made that the Internet be self-regulated. This means that people using the Internet would use their discretion when posting material, voicing their opinions and collecting data about people or other things. I believe many would agree that complete self-regulation on the Internet is nice in theory but unfortunately not pragmatic.

The legal system and society need to balance our 1st and 4th Amendment rights while still protecting our privacy. The legal system has a very difficult task in front of them.

To keep abreast of the developing Internet and legal issues there is a need to follow the latest news and legislation in the making. This will be an interesting way for students to learn about and to apply their knowledge of their 1st and 4th Amendment rights and to see how laws are made.

Lesson Plan # 1 - Department of Justice v. Cybercrime

What is being done to combat cybercrime?

Questions for Students:

What is meant by the term cybercrime?

Do you believe cybercrime is a problem?

What do you think is meant by the term cybercrime?

What type of people do you think are considered cyber-criminal?

What type of crimes do you think cyber-criminal commit?

Do you think you could ever be a victim of cybercrime?

Could a cyber-criminal invade your privacy?

Could a cyber-criminal steal your identity and personal information?

What do you think law enforcement officials are doing to protect the public from cyber-criminals?

Does cybercrime only effect people who use the Internet?

Objective: The students will research the following Justice Department web sites that describe what computer crime is and how to report it. The following web sites also include the latest thinking on privacy vs. policing on the Internet, and how the government searches and seizes computers.

Activity:

The student will choose at least two sites of interest to them from the attached list of web sites.
The student will view the site and take notes.

The student will explain the purpose of each site visited and relate it to the law, privacy and/or freedom of speech.

Students will share their findings with the class by giving a presentation on their 2 web sites.
Some overlap may occur, but this will help reinforce important issues with the class.
Students should include whether the topic is a privacy issue or a freedom of speech issue.

What the students will learn: students will learn about the different aspects of law enforcement on the Internet.

Materials to be used: Computers with Internet access, web site addresses, pen, and paper

@2H(after1H):The following is a list of web sites to be used in this lesson: Main Web page for the Department of Justice Cybercrime unit

<http://www.cybercrime.gov>

Reports, press releases, speech texts and testimony

<http://www.cybercrime.gov/doc.html>

Laws against computer crime and press releases on significant hacker cases

<http://www.cybercrime.gov/compcrime.html>

The agency's 200-page manual on prosecuting cases of intellectual property rights

<http://www.cybercrime.gov/ip.html>

Materials on electronic commerce and officials' testimony about Internet gambling and pharmaceutical sales

<http://www.cybercrime.gov/ecommerce.html>

Reports on the prosecution of Internet hate speech and cyber-stalking

<http://www.cybercrime.gov/speech.html>

Federal efforts to protect the national infrastructure that delivers essential services

<http://www.cybercrime.gov/critinfr.html>

Crimes facilitated by computer use

<http://www.cybercrime.gov/crimes.html>

The department manual on searching and seizing computers

<http://www.cybercrime.gov/searching.html>

Answers to frequently asked questions about encryption

<http://www.cybercrime.gov/crypto.html>

How to report privacy violations for investigation

<http://www.cybercrime.gov/privacy.html>

International efforts against computer crime and child pornography

<http://www.cybercrime.gov/intl.html>

Data on law enforcement cooperation against computer crime

<http://www.cybercrime.gov/enforcement.html>

Lesson Plan # 2 - Anonymous Speech, the Internet and Your Right to Privacy in the 21st Century

Should an individual have a “reasonable expectation of privacy” to remain anonymous and to voice their opinions, whatever they might be, and still be protected under the 1st and 4th Amendments?

Questions for Students:

What is meant by the term anonymous?

Have you ever sent or received an anonymous note or letter?

Why do you think Americans are granted the right of anonymous speech?

What are the benefits of anonymous speech?

What are the drawbacks of anonymous speech?

Objective: The students will learn about anonymous speech. We will research the reasons why anonymous speech is allowed in our country. We will look into what forums it is used today. And we will study and learn more about anonymous speech on the Internet, a person's right to free speech and freedom of expression in cyberspace.

We will study the case of John Doe v. Yahoo!.Inc. This is a current case (as of May 11, 2000) filed in United States District Court in Los Angeles by Aquacool_2000," a pseudonymous Yahoo! user. Yahoo! Inc. disclosed personal information about Aquacool_2000 to a company named AnswerThink Consulting Group, Inc. AnswerThink had subpoena Yahoo!

Under our 1st Amendment right, the Supreme Court in McIntyre v. Ohio Elections Commission, 414 U.S. 334 (1995) ruled that anonymity "is not a pernicious fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority." The Court pointed out that the U.S. has a long tradition of protecting the right to communicate anonymously, beginning with the Federalist Papers in the late 1700s. This Supreme Court decision upheld the right to distribute anonymous political leaflets.

Justice Oliver Wendell Holmes in McIntyre v. Ohio Elections Commission, said "Don't underestimate the common man. People are intelligent enough to evaluate the source of an anonymous writing. They can see it is anonymous. They know it is anonymous. They can evaluate its anonymity along with its message, as long as they are permitted, as they must be to read that message. And then, once they have done so, it is for them to decide what is 'responsible,' what is valuable, and what is truth."

Vocabulary: anonymity, pseudonymous, anonymous speech, plaintiff, defendant, complaint, invasion of privacy, breach of contract, negligence, unfair competition, false advertising, privacy policy, damages, compensation, injunction, defamation, subpoena, Internet, TRUSTe, personal information, internet protocol (IP),

Activity:

The students will explain what is meant by the term anonymous speech.

The students will give an example of when a person might use anonymous speech.

They will identify people, groups, or organizations, which might use anonymous speech.

The students will give examples why such people, groups or organizations would want to use anonymous speech.

The students will read the John Doe v. Yahoo case.

The students will look at the case from the employer's perspective.

The students will look at the case from John Doe's perspective.

As the lesson progresses students should give examples on when issues of privacy, freedom of speech, and contract law have been violated.

What the students will learn:

Students will be able to apply learned knowledge of the 1st and 4th Amendments to the Internet.

Students will learn about case law, tort law and the legal process.

Materials to be used: http://www.epic.org/anonymity/aquacool_complaint.pdf

http://www.epic.org/anonymity/aquacool_release.html

http://www.epic.org/anonymity/epic_aclu_release.html

Note:

With the passage of time, newer court cases and current event topics should be substituted.

Lesson Plan # 3 - Internet research on Your Right to Privacy

Questions for students

What do you think is meant by the term a reasonable “expectation of privacy”?

What type of information about you is actually private?

Are there any groups trying to keep your private information private?

How can you best protect your privacy?

Objective: The students will search the Internet for web sites that address privacy issues and the Internet. This may include web sites that focus on protecting an individuals right. Some of the best known groups include EPIC, EFF, ACLU.

Activity:

The students will choose at least two sites of interest to them.

The students will print out the web site text.

The students will read the text and take notes.

The students will explain the purpose of each site visited and relate it to the law, privacy and/or freedom of speech.

Students will share their findings with the class by giving a presentation on their 2 web sites. Some overlap

may occur, but this will help reinforce important issues with the class.

What the students will learn: students will learn about the different aspects of law enforcement on the Internet and about groups who help citizens protect their rights.

Materials to be used: Computers with Internet access, attached web site addresses, pen, paper

If students wish to conduct their own Internet search you might suggest the following key words. Also use these words to enhance vocabulary.

Internet	Privacy	Law	Constitutional Law
Encryption	E-mail	Cybercrime	Invasion of Privacy
Anonymous	Censor	Cookie	Legislation
Privacy & Security	Decrypt	Anonymous Remailer	Department of Justice

Lesson Plan # 4 - The 1st Amendment and Your Right to Free Speech and Privacy in the 21st Century

Questions for Students:

What are the four basic rights guaranteed to Americans by the 1st Amendment?

Why are these rights important to you?

What do 1st Amendment rights have to do with the Internet and privacy?

Should Internet users be able to say whatever they want on the Internet?

What if the subject is hateful, hurtful and offensive to most people?

Should web sites be able to include X-rated pictures and movies?

What types of laws should be made to protect minors from offensive material and text on the Internet?

What types of laws should be made regarding the topics we have discussed?

Should a person be able to hide their identity behind an E-mail address?

Allow for student discussion. This might include personal experience from Internet use and personal opinions.

Objective:

The student will demonstrate an understanding of the 1st Amendment and how their right of free speech is effected on the Internet.

The student will explain in writing what their first amendment right has to do with the Internet.

Activity:

The student will write a letter to their Congressperson expressing their thoughts on the Internet and their 1st Amendment rights.

The student might address subjects such as:

(Use these words to enhance student vocabulary.)

anonymous speech
pseudonyms
censorship
censorware or filtering software
encryption software
Internet Content Ratings

What the students will learn: The student will gain a better understanding about the 1st Amendment and how it applies to Internet users.

Materials to be used: web site addresses, pen, paper

Lesson Plan # 5 - The 4th Amendment and Your Right to Privacy

Questions for Students:

What is the 4th Amendment?
What does the 4th Amendment have to do with your right to Privacy? It doesn't say the word privacy.
What type of privacy should you expect in the workplace?
Can your employer read your E-mail on its corporate system?
What is a cookie? Do you eat this type of cookie?
Should businesses be able to track which web sites you visit on the Internet?
Should businesses be able to compile personal information about you?
Should businesses be able to sell to other companies your personal information?
What laws are there to protect you and your privacy?

Allow for student discussion. This might include personal experience from Internet use and personal opinions.

Objective:

The student will demonstrate an understanding of the 4th Amendment and how privacy is effected on the Internet.

The student will explain in writing what their 4th Amendment right has to do with the Internet.

Activity:

The student will write a letter to their Congressperson expressing their thoughts on the Internet and their 4th Amendment rights.

The student might address subjects such as:

(Use these words to enhance student vocabulary.)

E-mail
encryption
aggregating companies
cookies

What the students will learn: The student will gain a better understanding about the 4th Amendment and how it applies to Internet users.

Materials to be used: web site addresses, pen, paper

WEBSITES TO EXPLORE FOR TEACHERS AND STUDENTS

ACLU – American Civil Liberties Union

<http://www.aclu.org>

Center for Democracy and Technology – displays information gathered about you from your visit to this site.

<http://www.cdt.org>

For information on identity theft and how to protect yourself

<http://www.consumer.gov/idtheft>

Berkman Center for Internet & Society

<http://cyber.law.harvard.edu/>

Developments in the Law: The Law of Cyberspace

<http://www.harvardlawreview.org/issues/download/5-99-DEVO-III.htm>

Electronic Frontier Foundation

<http://www.eff.org/>

Encryption – Landmark Ruling

<http://www.wired.com/news/news/politics/story/19553.html>

EPIC – Electronic Privacy Information Center

<http://www.epic.org/>

FindLaw: Legal Subjects: Cyberspace Law Materials – Legal Documents

http://www.findlaw.com/01topics/10cyberspace/gov_laws.html

Free Email Services

<http://www.hotmail.com> or <http://www.mail.yahoo.com>

Internet Free Expression Alliance

<http://www.ifea.net/mission.html>

Internet Privacy New and Guides

<http://www.looksmart.com/>

Privacy Rights Clearinghouse

For information on the use of social security numbers look up #10

<http://www.privacyrights.org>

Smith, Quinn & Associates, PLLC Patent, Trademark & Copyright Law. This address provides educational materials and lists all U.S. Government branches and web sites. Legal Resources on the Internet

<http://www.sqlaw.com/resources.htm>

NYTimes Cyberlaw Journal

<http://www.nytimes.com/library/tech/reference/indexcyberlaw.html>

Ongoing Coverage of Internet Government Issues by the NY Times

(You must sign up for a free subscription to this site.)

<http://www.nytimes.com/library/tech/reference/index.domain.html>

ANNOTATED BIBLIOGRAPHY

For Teachers

Adamson, John E., Mietus, Norbert J. Law for Business and Personal Use 15th Ed. Cincinnati, OH South-Western Educational Publishing 2000

An up-to-date business law book with short segments addressing legal issues and the Internet.

Alderman, Ellen, and Caroline Kennedy. The Right to Privacy. New York: Vintage Books, 1997

This book is filled with interesting cases which address all types of privacy violations.

Congressional Quarterly Weekly Report, 01/31/98, Vol. 56 Issue, p237 4p

Congress Finds No Easy Answers to Internet Controversies

A report on the difficult issues Congress faces regarding the Internet.

Givens, Beth. The Privacy Rights Handbook. New York: Avon Books, 1997

This book provides an overview on how to safeguard your personal information and to protect your privacy from people and businesses. It also discusses rights a person has and what a person should do if their privacy has been violated.

Glass, Brett. "Keeping Your Private Info Private; Designing Privacy for Your E-Business; Utilities." PC Magazine June 6, 2000, pp. 118-139

A special report addressing Internet privacy issues regarding cookies, anonymous browsing, and protecting your privacy.

Hahn, Harley. Harley Hahn Teaches the Internet. Indiana; QUE, 1999

An easy to read and entertaining book teaching readers about the Internet and including ways to protect your privacy.

Mietus, Norbert, Adamson, John, Conry, Edward. Law for Business 14th Ed. Cincinnati, OH South-Western Publishing Co. 1993

A basic business law book beginning with information on our country's formation and the U.S. Constitution.

<http://www.cyber.findlaw.com/>

This site is designed as a resource for those interested in legal issues concerning cyberspace. Topics include commerce, cybercrime, freedom of expression, intellectual property, jurisdiction, privacy and general cyberspace law.

http://www.epic.org/free_speech/copa/ (5/17/00)

This web site is designed to inform browsers of the issues concerning your right to free speech on the Internet. It includes current topics and legislation.

<http://www.people.virginia.edu/~klb6q/infopaper/Workplace.html>

What About Privacy in the Workplace

<http://www.rbs2.com/privacy.htm> (5/23/00)

Ronald Standler writes an overview about Privacy Law in the USA.

<http://www.rbs2.com/ccrime.htm>

Ronald Standler addresses Computer Crime – Virus, Hackers, and Punishment.

<http://www.usdoj.gov/criminal/cybercrime/cyptfaq.htm> (5/31/00)

Department of Justice explains in detail their encryption policy. They cover three main topics: General Policy Issues, Law Enforcement Issues, and Constitutional Issues.

ANNOTATED BIBLIOGRAPHY

For Students

Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Vintage Books, 1997

This book is filled with interesting cases which address all types of privacy violations.

Givens, Beth. *The Privacy Rights Handbook*. New York: Avon Books, 1997

This book provides an overview on how to safeguard your personal information and to protect your privacy from people and businesses. It also discusses rights a person has and what a person should do if their privacy has been violated.

Glass, Brett. "Keeping Your Private Info Private; Designing Privacy for Your E-Business; Utilities." *PC Magazine* June 6, 2000, pp. 118-139

A special report addressing Internet privacy issues regarding cookies, anonymous browsing, and protecting your privacy.

Hahn, Harley. *Harley Hahn Teaches the Internet*. Indiana: QUE, 1999

An easy to read and entertaining book teaching readers about the Internet and including ways to protect your privacy.

Mietus, Norbert, Adamson, John, Conry, Edward. *Law for Business* 14th Ed. Cincinnati, OH South-Western Publishing Co. 1993

A basic business law book beginning with information on our country's formation and the U.S. Constitution.

http://www.epic.org/free_speech/copa/ (5/17/00)

This web site is designed to inform browsers of the issues concerning your right to free speech on the Internet. It includes current topics and legislation.

<http://www.usdoj.gov/criminal/cybercrime/cyptfaq.htm> (5/31/00)

Department of Justice explains in detail their encryption policy. They cover three main topics: General Policy Issues, Law Enforcement Issues, and Constitutional Issues.

<https://teachersinstitute.yale.edu>

©2019 by the Yale-New Haven Teachers Institute, Yale University

For terms of use visit <https://teachersinstitute.yale.edu/terms>