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

Invasion of Privacy--Has Cyber-Technology Made Privacy a Thing of the Past?

Curriculum Unit 00.03.01
by Valarie Arrington-Steele

Purpose

As a business teacher, I am currently teaching computer literacy. Part of the computer literacy curriculum includes teaching students how to access the Internet as well as being able to evaluate what you find online to make informed decisions to meet your needs. Students know that the use of computers is constantly growing and technology is incorporated in every aspect of our daily lives. What they also have to understand is that the convenience and hours saved by using computers or technology also sacrifices our privacy. The Internet is an open file of information. When an individual knowingly supplies personal information, they should know how that information is protected and used. They should also know how information that is not voluntarily supplied is collected and used.

Goals

This curriculum unit is a comprehensive, competency-based instructional tool designed to integrate the basic skills of reading, writing and computing, and the higher order skills of thinking, reasoning, problem-solving and decision-making. Its overall purpose is to teach students how their movements are tracked on the Internet and why. The goals of this unit are to provide students with the opportunity to:

Learn the basic components of online profiling
Learn about the mechanisms used to gather information and how they can control it
Learn the importance of reading and understanding privacy policies
Develop an awareness of agencies that have been set up to protect privacy rights
Develop an awareness of legislative issues.

The above goals will be accomplished by having the students access the Internet to view the cookie and web bug files that are used for profiling purposes, learn how to change cookie settings, evaluate privacy policies that they will get from the Internet, expand their Internet vocabulary and improve their collaborative problem-solving and critical thinking skills.. The students will also receive reading assignments and complete worksheets to further their understanding of existing laws and practices that are dealing with the privacy issue as it pertains to the Internet.

Everyone should understand that even when you browse the Internet in the privacy of your own home, some one could be watching your every move. No, they are not right there in the room with you looking over your shoulder, but every site that you visit, download or post messages to is being monitored. There is a saying "caveat emptorlet the buyer beware." It is time to apply that phrase to cyber-technology"browser beware."

Introduction

The Internet has been proclaimed to be the superhighway of the future. It is a convenience and also a necessity of the future. Many people have ambivalent feelings about this fast-growing technology that has endless possibilities but at the same time unforeseeable consequences. We are aware of computer crimes from hackers and other means, as well as problems like viruses, identity theft and pornography to name a few.

The Internet affects almost every aspect of our daily lives. We use it to shop, to apply for jobs, for artistic expression, business ventures, and for educational, medical, legal, and leisure purposes. It is a global infrastructure of communication networks, databases, computers and consumer electronics. With the capabilities of hardware, software, and communication networks continually increasing a nominal costs, information will be collected and used in ways that were previously impossible.1

Hence, information can now be acquired, processed, sent and stored easier, faster and cheaper. With continued advances in technology the collection, use and storage of information will become phenomenal.

The ease of collecting detailed personal information has made it possible for the collectors to share data between themselves for unrelated purposes. All of this in many cases is being done without the consent of the person whose information they are sharing.2

The convenience of using the Internet has seemingly made our lives easier, but at a major costthe lost of personal information privacy. The courts have recognized a basic right to privacy, a right to determine for ourselves how, when and to what extent our personal information is communicated to others. It is a basic, but not an absolute right. Of course, you have always had to supply personal information about yourself to get a bank account, driver's license, medical care, credit card, mortgage, etc., and this information was not completely private. But in the past, your personal information was not as easily accessible as it is now by the click of the mouse. Everything about you is stored in various databases on the Internet. Some of the information can be accessed by using a password, a social security number, and/or typing in your name at a particular web site. Some sites will charge you a fee and some are free. In other words, it doesn't take much for someone to have an extensive dossier about you.

You really had no control over offline information being placed on databases on the Internet, but they are now acquiring information for their databases from the information that you supply when you go on the Internet to communicate, order goods and services and obtain information. You are being trackedthis is called online

profiling. A profile is being set up about your browsing activities. Tracking on the Internet can tell what web sites you visit, what you bought, who you communicated with, when and for how long. You are tracked across shopping sites, news sites, leisure sites, general information sites and sites that you may not want anyone to know about.

Why is this being done? Because businesses say they want to learn more about their customers, develop better products to meet the needs of their customers, enter new markets and compete better. How do they do this? They track your behavior using pieces of codes called “cookies.”

Cookies

A “cookie” is a small data file that can be placed on your hard drive when you visit certain web sites. It is placed there by your Internet service provider, companies whose sites you visit, and banner ad companies.

A cookie contains a unique user name the Web site assigns to your computer. It is a text file on your computer that identifies your computer to the company that placed the cookie on your hard drive. 3

Every time you visit that site in the future, the site server will look for the cookie to provide information about your computer. A cookie’s purpose is to remember information. It can remember your log-in name or password at a particular site so that you don’t have to type it in every time you visit that site. It remembers the banner ads you have seen and the pages you visited at a particular site.

One server cannot read another server’s cookie or any other files on your computer, but (and there is always a but), if the sites form an alliance they can read another site’s cookie. If this happens, they are able to compile even more information about your browsing habits that are stored on their servers for future use.

According to consumer-advocacy groups, cookies were meant to be site specific. The ad networks are sharing the information found in cookies on the server side across multiple sites.4

The information on your cookie file is anonymous unless you have supplied personally identifiable information to a particular site. If the sites are sharing information, they can now put a name to the computer user who is visiting the music site, the sport site or some undesirable site you don’t want anyone to know about.

The ad agencies that supply the banner ads that pop up on your screen use cookies to help them determine what your interests might be as you move from site to site, and you will eventually start seeing banner ads related to your interests. One of the major advertising companies on the Internet is DoubleClick. Their privacy policy originally stated that they would not identify you personally. Unfortunately, DoubleClick was not happy having ads pop up on the screen to anonymous browsers so in June 1999, it purchased the direct-marketing firm Abacus Direct for $1.7 billion.

The purchase of Abacus gave DoubleClick the ability to cross-reference the 100 million cookies that it has set with the names, addresses, telephone numbers and purchasing habits of 90% of American households. All DoubleClick has to do is tie your cookies to the cookies of another site from which you have ordered a product or which requires registration to get positive identification and link that to its Abacus database. Privacy advocates are upset because DoubleClick refuses to say which sites are furnishing the registration information, and they believe the sites that are furnishing the information are probably violating the privacy

rights of the consumer. DoubleClick justified its actions by saying this will allow for more personalization of its online ads to better meet the needs of the consumer.5

Current statements on DoubleClick's Web site say it will notify the public before it starts merging the online and offline records by updating its privacy policy. Privacy advocates are concerned that even if they put a notice on their Web site, most of the people do not know that DoubleClick is the advertising company that supplies the ads or that their movements are being tracked by this advertising company.6

The good news is you can change the settings on your computer to accept cookies, not accept cookies or be prompted when a site is trying to send a cookie to your hard drive. When you use the prompt feature, you decide whether you want to accept or not accept a cookie at any given time. If your computer is set up to reject cookies, you may be denied access to certain web sites.

My computer uses Internet Explorer 5.0. To change the cookie settings, click Tools on the main menu bar, then click Internet Options, from this dialog box click Security, check to make sure the Zone in this dialog box is set to Internet, then click the Custom Level and scroll down until you find the Cookie section.

You can also delete the existing cookies on your hard drive. For Internet Explorer 5.0, go to Windows Explorer, click Windows in the C drive, click the Cookie folder, highlight the cookie or cookies you want to delete and hit the delete key.

Some sites will also use session cookies, "meaning that they are automatically deleted at the end of a session"7

In many cases you have control over the personal information that is collected based on the information that you personally supply when you order an item or service, register for contests, or sign up for free items or service. Your responsibility at this point is to know what information is absolutely necessary for you to supply in order to receive your request.

Teaching Strategies

In teaching this segment of the unit you will need to explain to students what online profiling is, why it is being done, and who is doing it. This can be accomplished by giving them a handout of detailed information that you have researched from periodicals, books, newspaper articles or Internet sites on information privacy. PC Computing and Smart Computing are excellent sources for information. The privacy advocate and "Cookie Central" Web sites are also invaluable sources for information. The "Cookie Central" Web site not only gives you valuable information about cookies, but it also allows your students to create a simulated tracking profile. You can also do a simulated tracking profile on the "Privacy.net" Web site. You should also show your students the cookies that have been stored on the school computer to give more credibility to the lesson. Students will be amazed at the number of cookies that have been stored on the computer. Also, have students check the cookie files on their home computers. Next, show your students how the cookie settings can be changed. Explain that being able to change the cookie settings, will give Internet surfers control over whether cookies are placed on their hard drives. Inform students that cookies can also be deleted from their hard drive at any time. (See Lesson Plan 1) You can also give students a written assignment to improve their writing, reasoning and decision making skills. Possible topics: (1) Are Internet cookies violating my privacy, or do they make

surfing easier? (2) Is profiling good or bad?

Privacy Laws and Principles

How is the information that has been obtained in previous offline databases and that which you have voluntarily supplied to online databases being used? What laws, rules or principles govern the Internet so that your personal information is not being misused and abused?

Abused by whomthe private sector or the government? It is the private sector; marketing firms and what is known as e-commerce and not the government that are moving by leaps and bounds to acquire and use personal information about individuals based on the almighty dollar.

The government at least has restrictions on how it can obtain information about you. The United States Constitution doesn't grant a right to privacy, but the Supreme Court has interpreted sections of the Constitution to protect different aspects of individual privacy. The Fourth Amendment provides the strongest protection which protects the right of the people to be secure in their persons, places, papers and effects from unwarranted searches and seizures by the government.8 Marketing companies don't need a warrant before they can create an online profile of you, but law enforcement agencies would need to obtain a warrant to tap into your online activities.

"The traditional rights of privacy focused on creating a zonea house or a personthat was protected from intrusion by the government except under specified circumstances."9 Privacy in the information age has been described as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others."10 "The laws of economics in the information age say that information has value,"11 and as long as Big Business can get away with self-regulation, they will rule. Why, because the "U.S. government does not have a legally enforceable privacy policy for the private sector,"12 and they are in no hurry to get one. According to Jaime Love of The Consumer Project on Technology, politicians from both parties are dragging their feet on the privacy issue because they want to continue to remain in the good graces of Big Business for the campaign contributions.13

The U.S. government has admitted that they do not want to stifle e-commerce, but there is a need for regulations that all companies must follow so there is consistency in what is acceptable and what is not. A lot of tracking is not disclosed and even if it is, it is being shared in many cases without consumer consent. The sharing of personal information is profitable to a business and to stay competitive more and more businesses will do it.

Some of the laws that have been passed include:

In 1966 Congress passed the Freedom of Information Act which provides a way for citizens to request information about the operation of government and what the government is doing with all the information it collects. The government does maintain the right to refuse to release information related to national security, intelligence activities, criminal cases and other areas.14

In 1972 the Advisory Committee on Automated Personal Data Systems to the Secretary of the Department of

Health, Education and Welfare stated basic principles for protecting privacy in the Information Age. They include disclosure of information-gathering activities, the right of individuals to correct information about them, and guarantees for accuracy and control of disclosure of information.15

The Privacy Act of 1974 was passed to make government agencies disclose their information-gathering and distribution activities and to give citizens the opportunity to learn what information has been collected about them and to correct any errors.16

The Electronic Communications Privacy Act of 1986 was passed to prohibit the unauthorized interception of all electronic communications stored or in transit to include computer data transmissions and e-mail.17

Congress also passed the Children's Online Privacy Protection Act of 1998 which prevents Web sites from gathering personal information about children without parental consent.18

We are a society that is accustomed to regulations; and with the Internet being as powerful as it is, and with the threat it poses to privacy and even our identity, it needs to be regulated. But the federal government is not ready to pass a lot of regulations governing online privacy. It argues along with big businesses that technology, namely, the Internet, is developing far too rapidly to be enclosed in a web of regulations.

President Clinton and Vice President Gore published a 21-page report entitled "A Framework for Global Electronic Commerce". It states:

> . . . Commerce on the Internet could total tens of billions of dollars by the turn of the century. For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce . . .
>
> Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act andat least as importantwhen not to act, will be crucial to the development of electronic commerce.
>
> In June of 1995, the Privacy Working Group of the United States Government Information Infrastructure Task Force issued a report entitled, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: Principles for Providing and Using Personal Information. The report recommends a set of principles (the "Privacy Principles") to govern the collection, processing, storage, and re-use of personal data in the information age . . .
>
> If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer

> choice regarding privacy online . . .
>
> The Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will re-evaluate this policy . . .19

Clinton does say the Privacy Working Group report recommends, and the key word here is "recommends," because what is recommended does not have to be followed, especially when big business is looking out for its own interest and how much money can be made in doing so. These guidelines are good but very basic in nature, and the committee does state that they have limitations and are not enforceable by law. The principles written to educate the private citizen should be taken to heart, because if we care about our personal information privacy we are the ones who will take this information seriously.

The PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION report published in June, 1995 by the Privacy Working Group clearly states:

> The "Principles for Providing and Using Personal Information" ("the Principles") are offered to respond to this new information environment. The Principles attempt to provide meaningful guidance.
>
> The limitations inherent in any such principles must be recognized. The Principles do not have the force of law and do not create any substantive or procedural right enforceable at law . . .20

The report outlines the general principles for all national information infrastructure participants, principles for users of personal information, principles for individuals who provide personal information and empowerment principles for individuals to safeguard their own privacy.

All of this, of course, sounds very good in theory or on paper if it were being properly practiced by the private sector on the various web sites, but that is not the case.

Teaching Strategies

For this segment of the unit you will need to review or teach students about the Fourth Amendment to the Constitution. It is important that you stress that although it does not grant a right to privacy, the Supreme Court has over the years interpreted various aspects of it to protect individual privacy based on changing social values, societal beliefs, and changing technology. Have students understand why the Fourth

Amendment was written by providing them with a short history of the public sector's need to be protected from government intrusion. To improve their reading skills have students read court cases that led to the various interpretations of privacy as it applies to this amendment as well as the legislation that has been passed to protect their privacy. To improve their thinking and reasoning skills, ask students for their opinions. Did they agree or disagree with the court decisions and why. Since the government has passed some laws on information privacy, you will need to explain to the students why it is in favor of self-regulation of Big Business on the Internet. You may want to review with them certain segments of the Clinton/Gore report and the Privacy Work Group "Principles". To improve their writing, reading, thinking, reasoning and research skills, have students write a paper. Possible topics: (1) Describe the application of the protections in the Fourth Amendment to modern information technology. (2) Describe the application of constitutional values and the argument for maintaining their integrity in confronting changes in technological capabilities. (3) Is self-regulation of Big Business on the Internet working in favor of the consumer as it relates to disclosure and consent?

EPIC--Privacy Advocate

The Electronic Privacy Information Center (EPIC) was established in 1994. EPIC strives to educate consumers on current privacy issues relating to the Internet. It produces reports conducts litigation, sponsors conferences, and publishes the EPIC Alert.21 EPIC believes that "online profiling is a serious threat to privacy because it happens so invisibly and information given to online companies can be used for a variety of purposes."22

In trying to educate consumers, EPIC published three reports. The first, in June 1997, was entitled "Surfer Beware: Personal Privacy and the Internet". This report reviewed the Internet privacy policies of 100 of the most frequently visited Web sites. The report found that only 17 of the sites had explicit privacy policies and none of the sites met the basic standards for privacy protection.23

The second report was published in June 1998, entitled "Surfer Beware II: Notice Is Not Enough." This report conducted the first evaluation of self-regulation to protect online privacy of 76 new members of the Direct Marketing Association (DMA). Forty of the 76 new members had Web sites and only 8 of the 40 had any form of a privacy policy. Of the sites that had privacy policies, only three had privacy policies that satisfied the DMA's requirements. None of the sites allowed individuals to gain access to their own information.24

The third report was published in December 1999, entitled "Surfer Beware III: Privacy Policies With Out Privacy Protection". This report reviewed the privacy practices of 100 of the most popular shopping Web sites to see if they complied with the set of principles recommended in the Privacy and the National Information Infrastructure Report on basic privacy protection, whether they used cookies, and if they used profiled-based advertising. The report found that 18 of the sites did not display a privacy policy, 35 of the sites used profile-based advertising and 86 of the sites used cookies. Not one of the sites adequately addressed all of the elements of the Principles and many of the sites' privacy policies were confusing, incomplete and inconsistent.25

David Sobel, General Counsel for EPIC believes that Internet users should not have to depend on the various privacy policies of every Web site. The government needs to establish basic guidelines and ground rules that apply from one site to another.26

Teaching Strategies

There are many privacy advocate groups, and I have given you a list of some of them at the end of this unit. I chose to focus on EPIC because of the three reports that they published on privacy policies over a three-year period. To teach this segment, explain the purpose of privacy advocate groups to your students and supply them with a list of these groups. To improve their reading skills, you can have them visit the Web sites of two or more of these groups to get more detailed information about their statement of purpose as well as reading the current news on privacy issues from an advocacy point of view. To improve student writing and critical thinking skills, have them write a short report about their opinions on two of the privacy issues that they read about. You can also have the students visit the Web site periodically and give an updated report on the two privacy issues that they originally chose to report on and/or have them report on new issues.

Privacy Policies

A privacy policy should describe and give specific details about how a Web site gathers information and how that information is disseminated. The Web site should put a link to their privacy policy on the home page where it is easy to find, and if the Web site shares information with a third party, you should be made aware of that and given the opportunity to restrict such use.27

One of the major problems facing consumers is that many of them do not read the privacy policies of the various web sites and many consumers might not even realize that each Web site has or should have a privacy policy. While researching this topic, I informally asked 45 adults if they read the privacy policies on the various web sites that they visited, and they all said “No.” Fifteen of them said they knew the policies were there, but they just did not read them. The other 25 said they never paid attention to the site for that type of information. I asked my students if they knew about privacy policies on the Internet, and they did not have any idea what I was talking about. Obviously, consumers need to be educated for their own protection.

If you do know about privacy policies, what should you be looking for that will protect your rights? As the EPIC report states, privacy policies can be confusing, incomplete and inconsistent.

In researching this unit, I have read a lot of privacy policiessome good, some not so good. Many of them tell you why personal information is collected, how it is used, what information is shared with their partners or sponsors (although they do not tell you who their partners or sponsors are), and what non-identifying information is shared with online advertisers (third parties). Some will tell you that they track your movements using cookies. Some were cagey enough to say they do not use cookies, but that they do track you (the question is-- How?). As I mentioned in the section called “Cookies,” a site will tell you that they use cookies; but they won’t tell you that they may form an alliance with other sites to read their cookies. Other important information that was explained in some privacy policies and not in others was: the ability to update or correct personal information, the security measures that they have in place to protect your information, that they do make revisions to their privacy policies, how you can receive information about updated services or products, and the opportunity to opt-out or opt-in to supplying certain information about yourself.

> . . . many Web sites follow an “opt-out” policy, in which information about a site visitor is automatically collected unless the visitor specifically requests it not be.28

Last but certainly not least, a statement telling you that no transmission over the Internet can be guaranteed to be 100% secure. Even though companies strive to protect your personal information, you transmit information to them at your own risk. Once that information is received, they will do their best to secure it.29

It all boils down to you, the consumer, deciding what information you want to supply to these Web sites for the services or products you want to receive. Although the privacy policies may not be perfect, they do provide you with much needed information to make an informed decision.

Teaching Strategies

Hand out a privacy policy from a Web site on the Internet and explain the content areas as well as why they should take the time to read privacy policies. You may also want to give students a glossary of terms that apply to privacy policies. Some privacy policies are short and some are very lengthy in their explanations. You should compare and contrast the content areas of at least two. To have students demonstrate an ability to work cooperatively with peers by communicating thoughts and ideas to justify a position, have them work in small groups to evaluate a privacy policy. The evaluation of privacy policies will also improve their critical thinking skills as well as teach them evaluation skills that they will need to develop in this technological age with an evolving online world with nonexistent standards. Supply students with a worksheet to guide them in the evaluation process. (See Lesson Plan 2) To improve oral communication skills, brainstorm with your students about the general principles of privacy, information integrity, and accuracy that should guide privacy policies and regulations. To improve their decision-making skills and challenge their thinking, have students work in small groups as a legislative body to come up with basic guidelines and ground rules that should govern all privacy policies.

TRUSTe

E-commerce has set up its own watchdog. The organization is called TRUSTe. TRUSTe has been in existence for three years. TRUSTe was set up to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. When a site displays a TRUSTe seal, it is saying that it will notify its customers of what information it is tracking, how it is using the information, and what companies it shares the data with.30

TRUSTe actively encourages and helps businesses institute voluntary privacy policies and statements. However it has no authority to mandate the policies, or does it ensure the policies provide a minimum level of personal-information privacy protection.

The fact that e-commerce does not always abide by the rules of the TRUSTe organization is the reason privacy advocates are complaining. They feel that members of TRUSTe are inadequately monitored, and it has been the consumers and privacy advocates that actually report violations. Once the violations are reported and receive press coverage, the companies change their privacy policies.31

Even though President Clinton has concerns about online privacy, he still believes in e-commerce self-regulation based on the statement he made in a press release on March 6, 2000. The President urged online

business leaders to improve privacy protection on the Internet by challenging the Internet companies to engage in effective self-regulation by participating in programs like TRUSTe.32

TRUSTe has recognized that there is a problem especially with third party ad servers. In a press release on March 7, 2000, it announced the formation of an Advisory Committee to consider its requirements and the challenges they pose to licensees engaging the services of third party ad servers. The committee is comprised of experts from inside and outside of the Internet industry. Their goal is to arrive at a comprehensive set of recommendations that represent the many aspects of the privacy discussion.33

On July 25,2000 TRUSTe kicked off its Privacy Partnership 2000 campaign along with 12 of the most recognized Internet companies. The campaign is designed to educate and empower consumers to control their personal information online. The public will be notified about the campaign through banner ads, radio public service announcements, and print advertisements that will run throughout the month of August in 26 major metropolitan publications.34

TRUSTe can only recommend what commercial Web sites should do to protect consumer privacy. It is up to businesses to answer to consumer privacy concerns directly, honestly and effectively.

Teaching Strategies

In teaching this segment of the unit, have your students visit the TRUSTe Web site to read and learn more about this organization. The Web site has a privacy glossary of commonly used privacy and related Internet terms. The site suggests consumer do’s and don’ts about cookies, privacy statements, seal programs, etc. There is an excellent privacy challenge quiz consisting of 12 multiple choice questions dealing with privacy policies, software, password protection, etc. The site suggests privacy protection guidelines that they encourage you to print out and keep next to your computer, and there is a section on government activities.

Conclusion

Privacy on the Internet is a very broad issue. This unit only explains a few of the things that you can do to protect your own personal-information privacy while using the Internet and what you can teach your students.

What should your students get out of this unit? The ability to be able to participate in an informed manner what information they want Web sites to have about them, how that information is used, and how that information is protected. Read books, access the Internet, etc., to become aware of current issues about privacy rights and gain an understanding of such rights in order to speak intelligently on the impact to consumers, businesses and the government. Summarizing information from reading material by clearly and succinctly articulating its major points and proposals. They should also realize that the major threat to privacy today comes from big business, not the government.

Reading privacy policies are very important because each site’s policy is a little different depending on what they have or have not included. For example, why they are collecting information, how different sites share their data, which sites are members of TRUSTe, how you can update your information and how and why your personal information can be shared with law enforcement agencies if the law allows it.

Make your students aware of advocacy groups that are fighting for their privacy rights and the various laws that have been passed to protect their privacy as well as the government's hesitancy to regulate such a dynamic infrastructure. Explain the Fourth Amendment to them so that they fully understand where this country started in our quest for privacy and how the Constitution is constantly being reinterpreted to meet the needs of changing lifestyles, changing technology and changing times.

Of course, there are many others ways to protect your privacy online. Hopefully this unit has piqued your interest, and you will want to do further research.

Endnotes

1Privacy Working Group, "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information." HYPERLINK http://www.iitf.nis.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html http://www.iitf.nis.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html. June 6, 1995. 2CDT's Guide to Online Privacy, "Chapter Three: Existing Privacy Protections and Initiatives."

http://www.cdt.org/privacy/guide/protect/.

3Michele Nelson, "Web Tracking Is Watching You." Smart Computing, vol. 8, issue 4, p. 21. 4Jennifer Farwell, "Online Profiling." Smart Computing, vol. 8, issue 4, p. 25. 5Will Rodger, "Activists Charge DoubleClick Double Cross."

http://www.usatoday.com/life/cyber/tec/cth211.htm. February 21, 2000.

6Leslie Miller and Elizabeth Weise, "FTC Studies Web Site 'Profiling'."

http://www.usatoday.com/life/cyber/tech/review/crg570.htm. November 23, 1999.

7Privacy Policy for AllAdvantage.com.

http://www.alladvantage.com/privacy.asp. August, 1999.

8CDT's Guide to Online Privacy, "Privacy Basics."

http://www.cdt.org/privach/guide/basic/

9Harry Henderson, Privacy in the Information Age. New York: Facts On File, Inc., 1999. p. 16. 10Fred H. Cate, Privacy in the Information Age. Washington, D.C.: Brookings Institute Press, 1999, p. 22. 11William Wresch, Disconnected Haves and Have-nots in the Information Age. New Brunswick, NJ: Rutgers University Press, 1996, p. 93. 12Jeff Dodd, "Us vs. Them." Smart Computing. vol. 8, issue 4, p. 10. 13Michael Sweet, "Protecting Privacy in a Digital World." Smart Computing, vol.8, issue 4, p. 8. 14Marc Rotenberg, Privacy Law Source Book 1999, United States Law International Law and Recent Developments. Washington, D.C.: EPIC, p. 57. 15Marc Rotenberg, p. 65. 16Marc Rotenberg, p. 38. 17Marc Rotenberg, p. 103. 18Marc Rotenberg, p. 165. 19President William J. Clinton and Vice President Albert Gore, Jr., "A Framework for Global Electronic Commerce." http://www.iiff.nist.gov/eleccomm/ecomm.htm 20Privacy Working Group 21Electronic Privacy Information Center. HYPERLINK http://www.epic.org http://www.epic.org. 22Michael Sweet, p. 6. 23EPIC, "Surfer Beware: Personal Privacy and the Internet."

http://www.epic.org/reports/surder-beware.html,.June 1997.

24EPIC, "Surfer Beware II: Notice Is Not Enough."

http://www.epic.org/reports/surder-beware2.html, June 1998.

25EPIC, “Surfer Beware III: Privacy Policies Without Privacy Protection.”

http://www.epic.org/reports/surfer-beware3.html, December 1999.

26Ed Bott, “We know Where You Live, Work, Shop, Bank, Play, and So Does Everyone Else.” PC Computing, vol. 13, March 2000, p. 82.

27Privacy Choices, “Understanding Your Rights.”

http://www.privacychoices.org/content_understanding.htm.

28Privacy Choice, “Opt Out.”

http://www.privacychoices.org/content_optout.htm.

29Yahoo Privacy Policy.

http://docs.yahoo.com/info/privacy/ p. 8.

30TRUSTe, “TRUSTe Approves 1000th Web Site.”

http://www.truste.com/about/about_1000th.html.

31Daniel Tynan, “Privacy 2000, In Web We Trust?” PC World, June 2000, p. 116. 32TRUSTe, “President Clinton to Industry: Join TRUSTe.”

http://www.truste.com/about/about_clintonspeech.htm.

33TRUSTe, “TRUSTe Forms Advisory Committee on Third Party Ad Servers and Licensee Practices.” http://www.truste.com/about/about_tpas.html. 34TRUSTe, http://www.truste.com

Lesson Plan 1

Objectives:

The st udent will access the cookie folder.

The student will read a cookie file and determine which site sent it.

*The student will be able to delete cookies.

*The student will be able to change cookie settings.

*Since this is being taught at school, you do not want to delete or change the school settings, just show the students how it can be done.

Viewing a cookie file

To access the cookie folder for Internet Explorer go to Windows Explorer, scroll down to the C drive and click Windows in the C: listing, find the Cookie folder and click, the cookie files will be listed.

To access the cookie folder for Netscape Navigator go to Program Files, click Netscape, then click the Users folder, and scroll down to the Cookie folder and click.

Since this is being done at school, the cookie listing will be very long. This gives students a good indication of the number of cookies that are placed on a school computer everyday. Make students aware that individual profiling is not possible, but aggregate profiling is. Students should see banner ads that are tailored to students.

Once students are in the cookie folder have them identify five or more sites that may be familiar to them. Recognizing the name of the site is very easy.

Next, make sure you have their undivided attention. Tell them that you are only going to explain to them how to delete a cookie file. They are not going to physically delete a file.

Explain to students that they can delete any or all of the cookie files in the folder by highlighting the file and pressing delete. It's that simple.

Changing cookie settings

Again, tell your students that you are just explaining to them how to change the settings, they are not going to physically change them.

On Internet Explorer select Tools on the main menu bar, click Internet Options, click Security, check the zone to make sure it says Internet (if it doesn't, change it), then click Custom Level, scroll down until you find the Cookie section. It will say enable, disable or prompt. One of these will be checked.

On Netscape Navigator select Edit from the main menu bar, click Preferences, click Advanced, scroll down to the Cookie section. It will say accept, disable or warn.

Now tell your students if they have a computer at home and are connected to the Internet, they can become the teacher. If their parents do not know about cookies, they can teach them. Tell them to get their parent's permission before deleting or changing the cookie settings on their computer.

Students learn by doing and learn even more when they teach it to someone else.

Lesson Plan 2

Objectives:

Students will evaluate privacy policies.

Students will utilize critical thinking skills.

Students will work collaboratively and individually.

The purpose of this lesson is to make students aware of privacy policies, how they should evaluate a policy as well as improving their reading, writing, and critical thinking skills.

Teaching students evaluation skill for online activities where there are no regulatory standards is a major component of computer literacy. The students must be challenged to think and to express themselves.

Explain what privacy policies are to your students. Hand out a privacy policy and explain the content areas.

Provide students with a glossary of Internet terms that pertain to privacy policies. For example--informed consent, opt out, secondary use, aggregate, access, disclosure, cookie, third party, server, encryption, usage data, sponsors, and TRUSTe.

Prepare a worksheet for students to use as a guide so they will know what should be included in a privacy policy.

Sample Worksheet Questions

Is there a link for the Privacy Policy on the site's home page?

Does it tell you why the data is being collected?

Does it tell you how the data is being collected?

Does it tell you how the date will be used?

Does it tell you what information is supplied to third parties?

Does it tell you how your information is protected?

Does it tell you how to change or delete your personal information?

Is the site a member of TRUSTe?

Is the content of this page appropriate for you to make an informed decision?

Is there information that contradicts something you found somewhere else in the policy?

Is there a date of last update?

Does up-to-date information matter to you?

Is there any information on the page that you disagree with?

Do they use absolute words (like "always" or "never")?

Would you do business with this Web site?

Have the students form groups of three or more depending on the size of your class. Give each group a

privacy policy from one of the top Internet service providers (i.e. AOL, Microsoft).

I think students should work in small groups to evaluate their first privacy policy. It makes it easier, and it also gives them the opportunity to work collaboratively to solve a problem. This is being done many times in real-life situations.

Once the students have completed the worksheet, have them formulate and justify their ideas by writing a narrative evaluation.

Example of narrative evaluation

After answering all of the questions on the worksheet about this privacy policy, explain why you think this is or is not a good privacy policy.

Letter

You can also have the students write a letter to the company. Have them tell the company what they think the company should include in their privacy policy and why it should be included.

For the last phase of this lesson, have students work individually. Have them pick a privacy policy from a Web site of their choice. Follow the same procedures that were used above.

Lesson Plan 3

Objectives:

Students will learn about the privacy concerns of advocacy groups.

Students will learn about current legislative issues.

Give your students a questionnaire about their views on privacy.

Example

What is your privacy worth?

What information about you or your parents do you think should be considered private?

Why are issues of personal-information privacy so important today?

On a handout cite the Fourth Amendment to the Constitution. Cite a few cases that have changed the interpretation of how privacy is applied to this amendment. (i.e. Roe vs. Wade). List the advocacy groups that are concerned about privacy issues and their purpose. Explain the government's position on not regulating e-

commerce.

Next have students go to two or more of the privacy advocate Web sites. Have them read about current legislative issues, current press releases and other pertinent information about these organizations. Have students write a report on their findings.

Do a follow-up questionnaire.

Example

Where should we draw the line between privacy and the common good?

What do you think is the “Privacy Paradox’?

Where do you think the major threat to privacy today comes fromgovernment or big business?

Do you believe that in order to protect our privacy, regulations are necessary?

Is privacy even possible in the new millennium?

Is privacy a commodity rather than a right?

Is technology changing our understanding of what is private?

Materials to be Used

Computer with Internet access

Internet Web sites

Books, newspaper articles, and magazine articles relating to privacy issues

Paper, pen and/or pencils

@SH:Bibliography (Teachers)

Agre, Philip E. Technology and Privacy: The New Landscape. MIT Press, August, 1998. (A collection of essays representing European, Canadian and U. S. points of view on how technology is changing our understanding of what is private). Alderman, Ellen and Caroline Kennedy. The Right to Privacy. Vintage Books, February, 1997. (An excellent book on privacy cases). Branscomb, Anne Wells. Who Owns Information: From Privacy to Public Access. Basic Books, April, 1995. (A useful book about the ownership of information). Cate, Fred H. Privacy in the Information Age. Washington, D.C.: Brookings Institution Press, 1999. (Impact of technology on information privacy) DeCew, Judith Wagner. In Pursuit of Privacy: Law Ethics and the Rise of Technology. Cornell University Press, June, 1997. (Legal discussions on the right to privacy and how it should be guaranteed in various contemporary contexts). Etzioni, Amitai. The Limits of Privacy. Basic Books, April, 2000. (Discusses why the main danger to privacy comes from the private sector). Garfinkel, Simson and Deborah Russell. PGP: Pretty Good Privacy. O’Reilly & Associates, Inc., January, 1994. (Technical user’s guide about cryptography and privacy). Garfinkel, Simson and Deborah Russell. Database Nation: The Death of Privacy in the 21st Century. O’Reilly & Associates, Inc., January, 2000. (Explores today’s threats to privacy and how they might be stopped). Gelman, Bob and Stanton McCandish. Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace. Harper Collins Publishers, Inc., January, 1998. (Good guide to self-protection on the Internet) Henderson, Harry. Privacy in the Information Age. New York: Facts On File, Inc., 1999. (Tells about

the impact of technology on information privacy). Pfaffenberger, Bryan. Protect Your Privacy on the Internet. Wiley, Jojn & Sons, Inc., April, 1997. (Informs you about software and information necessary to protect yourself on the Internet). Rotenberg, Marc. Privacy law source Book 1999: United States law, International Law and Recent Developments. Washington, D.C., EPIC (Excellent book on privacy laws and issues). Smedinghoff, Thomas J., Andrew R. Basile, Geoffrey G. Gilbert, and Lorijean C. Oei Strand. Online Law: the SPA's Legal Guide to Doing Business on the Internet. Addison Wesley Longman, Inc., January, 1995. (A reference book about how the law applies to the online world). (Students)

Alderman, Ellen and Caroline Kennedy. The Right to Privacy. Vintage Books, February 1997. (An excellent book about privacy cases). Gelman, Bob and Stanton McCandish. Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace. Harper Collins Publishers, Inc., January, 1998. (Good guide to self-protection on the Internet). Gottfried, Ted. Privacy: Individual Right vs. Social Needs (Issue and Debate). Brookfield, CT: Millbrook Press, 1994. (Discusses court cases and issues conducive to high school age readers). Hendricks, Evan, Trudy Hayden and Jack D. Novik. Your Rights to Privacy: A Basic Guide to Legal Rights in an Information Society. (An American Civil Liberties Union Handbook). Carbondale, IL: Southern Illinois University Press, 1990. (Provides guidelines to individual rights to privacy using a question and answer format). Noon, E. Personal Privcy Protection Guide: A Practical Guide to Protecting Your Privacy. ONOne, Inc., June, 1998. (Good guide for protecting your privacy). Sykes, Charles J. The End of Privacy. St. Martin's Press, Inc., September 1999. (Traces the roots of privacy from the Constitution to present day).

Internet Sites That You May Find Useful In Your Classes:

This site gives you a glossary of Internet terms. CDT's Guide to Online Privacy – http://www.cdt.org/privacy/guide/terms/ Teachers First – http://www.teachersfirst.com/glossary.htm This information can be accessed by anyone. It is free and it will show your students a small fraction of the large databases that are on the Internet.

White Pages – http://www.whitepages.com (offers more than 100 million listings, it will also supply you with a map and directions to a particular residence)

AT&T'S Directory Anywho – http://www.anywho.com (directory that also tells you who else lives on a particular street) Information Directory – http://www.555-1212.com (offers a celebrity directory as well as telephone listings for 100 million residences and 2 million businesses and e-mail) Reverse Directory – http://www.reversephonedirectory.com (offers reverse telephone look up) E-mail Addresses – http://www.bigfoot.com (offers 35 million e-mail addresses) This site will tell you some of the software that is out there to protect your privacy. Privacy-Related Software – http://privacy.net/software/ This site gives an excellent example of how banner ad networks track your movements on the Internet. Privacy.Net – http://privacy.net/cookies Cookie Central – http://www.cookiecentral.com This site gives you a list of the major Internet service providers.

Infoplease.com – http://www.infoplease.com/ipa/A0151967.html This site gives an excellent example of what information is collected about your computer when you go online. Snooper 2.0 – http://snoop.cdt.org/ These sites deal with privacy issues. American Civil Liberties Union – http://www.aclu.com Electronic Frontier Foundation (EFF) – http://www.eff.org Information Systems Security Association – http://www.issa_intl.org Institute of Electrical and Electronics Engineers (IEEE) – http://www.ieee.org Internet Society – http://www.isoc.org Privacy Rights Clearinghouse – http://www.privacyrights.org This site tells you the top 10 ways to protect privacy online. CDT'S Guide to Online Privacy -- http://www.cdt.org/privacy/guide/basic/topten.html