ETHICAL ISSUES IN WEB DESIGN

Dr. James K. Harris  
Department of Computer Sciences  
Georgia Southern University  
Statesboro, GA 30461  
912-478-CSCS  
jkharris@georgiasouthern.edu

ABSTRACT

This paper explores the meaning of ethical Web design. It defines a set of guidelines as to what could help define ethical Web design and gives real world examples for justification. These examples provide excellent case studies for a Web design class.

Keywords: Web design, Ethics, Privacy.

INTRODUCTION

Ethical issues involving Web design are not yet well defined. One of the intents of this paper is to help define the meaning of ethical Web design through design guidelines and to give real world examples that motivate the establishment of the proposed guidelines. These guidelines and examples can be used in Web design courses to help maintain awareness of ethical design issues students are likely to face as Web designers.

ETHICAL WEB DESIGN

Ethical principles for a profession are described in a set of guidelines or codes. One criterion for establishing a set of ethics guidelines for Web design should be consistency with established ethical guidelines for software engineering, namely, the ACM-IEEE Joint Software Engineering Code of Ethics (JSECOE). The first JSECOE code states “Software engineers shall act consistently with the public interest”. The second code

* Copyright © 2009 by the Consortium for Computing Sciences in Colleges. Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the CCSC copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Consortium for Computing Sciences in Colleges. To copy otherwise, or to republish, requires a fee and/or specific permission.
states, “Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest”. So according to the JSECOE, the public interest is first and foremost. The question now becomes, “How should a Web site be designed so that it is in the public interest?” Since the JSECOE is a normative code, four broad ethical Web design guidelines are proposed to be included into what constitutes the “public interest”. These are:

1. Information should not be hidden
2. Information should not be used or transferred without proper consent
3. Consent should be properly obtained
4. Privacy should be maintained

**HIDING INFORMATION**

Important information on a Web site should be easily accessible from the main page. Whether through poor or intentional design, many Web sites hide important information. Web designers often hide important information by using non-prominent links and burying it multiple links down from the main Web page. Yahoo!’s cookie policy page described later in this paper is a great example of how this is done. A more subtle design problem is the misuse of display formatting objects. For example, HTML text areas are often used to display important information. Google’s “Terms of Service” agreement on their “Create a Google Account” Web page [2] is displayed on Google’s Web site in an HTML text area (Figure 1).

![Google Terms of Service](image)

**Figure 1: Googles “Terms of Service” Text Area**

The text inside the text area for the Terms of Service is 541 lines long, but the text area only displays 10 lines at a time. The user must scroll through the text area to see the other 531 lines. This is a classic case of hiding important information from the user. A much more responsible design would have the Terms of Service text spread out over an entire Web page with carriage returns at the visible edge of each line. Google does use this design on other Google pages [6], but not on their Sign-up page, where the Terms of Service information is critical for the user to make an informed choice. Yahoo! also uses the latter design [7]. A design mistake similar to the misuse of text area containers
is the misuse of multiple frames. Each frame can hide important information by forcing the user to scroll through a Web page much larger than the containing. An even worse problem is the use of pop-up windows to display important information. If the user’s browser blocks pop-up windows, or scripting is turned off in the browser, the information will never be displayed. In the former case, the user can usually view the pop-up window by giving consent, but in the latter case the user may never even know they missed the information. In fact, there are so many different ways to display information on Web pages that users may not even be aware of how to access the information. A text area inside of a frame on a pop-up window might force the user to give consent to view the pop-up, scroll to find the text area within the frame and then scroll within the text area to find the information.

TRANSFER & USE OF INFORMATION

An issue that presents itself in a Web design course is the transfer of information from the user’s computer to another computer. Information is most often sent from the browser to the server through form fields. Most form fields contain information entered by the user, however, form fields can be hidden and populated by JavaScript or other client-side scripting languages with data collected from the user’s computer. When a form is submitted to the server, the information in hidden form fields is also sent. It should be emphasized to students that sending information, especially non-technical information, in a “hidden” manner, such as hidden form fields, without explicitly notifying the user that this transfer is taking place, is ethically irresponsible. In an ethically responsible Web site, all data transferred from the client to the server should be explicitly described in the privacy policy. What data is being sent, how it will be used, how long it will be kept should all be explicitly stated in the policy. When a simple Web form, written using HTML, is submitted, the user is aware of the submission as the Web page is “refreshed” by the server. In the case of newer technologies, such as AJAX, this is not the case. A form submission may occur without any noticeable change in the page displayed by the browser. This allows code within the browser to send information from the browser to the server without any knowledge by the user that a transfer is taking place. When introducing technologies such as AJAX in Web design classes, students should be made aware of the privacy implications. An ethically responsible design would allow the user to be able to view the information that is to be transferred before the transfer is made and the user should be able to decide what data is transferable. One way to implement this scheme is to provide a link on the Web page that when clicked, displays the data to be transferred in a readable form in a new window with the choice of opting-in to allow the transfer of each datum. Unfortunately, rarely, if ever, are these features designed into Web pages. The previous transfer issues dealt with transferring information from a Web site. There is also the ethical design issue dealing with improperly importing data into a Web site. For example, news feeds from a legitimate Web site can be stripped and posted on a separate site with its own advertisements. Finally, proper consent should be obtained before collected information is used. This is, again, a normative guideline and should spark debate as to what is “proper”. For example, is it proper for a Web designer to have a blanket statement such as Yahoo!’s “We limit access to personal information about you to employees who we believe reasonably need to come into contact
with that information to provide products or services to you or in order to do their jobs.

**OBTAINING PROPER CONSENT**

Obtaining consent from the user of a Web page should be done in an honest and straightforward manner. Consent on Web pages is usually obtained in one of four ways:

1. The policy is stated and consent is assumed;
2. opt-out;
3. opt-in;
4. opt-in for the initial consent and for consent for each secondary use, disclosure, or transfer of data.

If the policy is stated and consent is assumed, the policy should be stated in a prominent and easily accessible area on the Web site and not hidden in an obscure area. By itself, assumed consent is not legally binding. This is why assumed consent is usually tied to a user action, such as the installation of software, essentially making it opt-in consent. Opt-out consent requires that the user perform an action in order to remove consent (such as un-checking a checkbox). Opt-out checkboxes are very often placed on Web pages in non-prominent positions in order to solicit consent without the user knowing that the check box is checked. It should be emphasized to students that opt-out is for the most part a dishonest and unethical way of obtaining consent. A good example of abuse of opt-out comes from the “Create a Google Account” Web page just off the main Google page.

According to Google’s Web History FAQ page:

*In order to provide the service, Web History saves information about your web activity, including pages you visit and searches on Google. Over time, the service may use additional information about your activity on Google or other information you provide us in order to deliver a better search experience.*

The information collected is not anonymous. It is tied to the user’s computer through their IP address and their Google account:

*To use Web History, you'll need to register for a [Google Account](https://accounts.google.com). At that time, we'll ask you for some limited personal information, including your email address and a password which we'll keep on our system in an encrypted form.*

None of this information is on the main Google Sign-Up page with the opt-out checkbox. In fact, to find the Web History FAQ page it was necessary to do a Google search! The use of opt-out in this example is unethical. Using high profile Web pages such as Google and Yahoo! helps to drive home these points to students. Another problem with opt-out consent is when a form is incorrectly submitted. When a Web form is incorrectly filled out very often the Web server will repost the original page with the
opt-out consent set. It will then be necessary for the user to opt-out again. This is easily overlooked and consent could be given without knowledge. Opt-in consent requires that the user perform an action in order to give consent (such as checking a checkbox). In most situations, opt-in consent is considered a more ethically responsible way of obtaining consent rather than using opt-out consent. However, many Web sites turn opt-in consent to opt-out consent using the negation of a statement. For example, “Check here if you do not wish to receive our newsletter”. This is even less ethically responsible design than using opt-out check boxes. The request becomes obfuscated using the negation. Also, it should be noted that when opt-in consent is given, the consent might apply to secondary uses of data. Ethically responsible design requires that all secondary uses of data should be clearly presented on a Web page at or near the location of the opt-in consent. Opt-in consent for each secondary use, disclosure, or transfer of data protects the rights of the user, but even this type of consent has problems. If the user must perform opt-in consent many times due to policy changes or multiple secondary uses, there is a tendency to opt-in without reading the updated consent agreement or secondary use. Changes to consent agreements can be done in a similar fashion as the initial consent agreement. Either the consent can be posted and it is the responsibility of the user to read the changes, the user is notified of changes and must opt-out of the new agreement, the user is notified of the changes and must opt-in to the new agreement, and the user is notified of the changes and must opt-in for the new agreement or any secondary use, disclosure or transfer of data. An ethically unacceptable design, which happens all too often, is when the changes are posted in an obscure area of a Web site and it is the user’s responsibility to regularly check the site to view new changes. Some Web sites even go as far as moving changes to consent agreements regularly within the Web site in order to “hide” the changes. A more responsible scheme is to directly notify the user of the changes and allow them to opt-in to the new consent agreement. Yahoo!’s change of policy is shown below [5]:

Yahoo! may update this policy. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your Yahoo! account or by placing a prominent notice on our site.

Google has a similar policy. The problem with this is that both Yahoo! and Google get to define what a “significant change” is. Also, contact information is not always available for each user. However, users can be notified by storing information in a cookie identifying which version of the consent agreement was agreed upon by the user. The user can then be notified the next time they visit the Web site that the consent agreement has changed and be allowed to opt-in to the new consent agreement or cancel the agreement.

MAINTAINING PRIVACY

When designing Web sites, students should be made aware that special consideration regarding privacy should be placed on the storage and transfer of personal information. As discussed previously, current Web technologies allow for the storage and transfer of information from the client to the server without the client’s knowledge or consent. Client side cookies are small files that are created in a scripting language such
as JavaScript. Each cookie usually has a maximum size of 4096 bytes (4 KB). Each server can create at most 20 cookies for a total of 80 KB of total cookie space per server. Cookies are only supposed to be able to be accessed by the hosting server that created the cookie using the servers IP address as identification. There are many legitimate uses of cookies. For example, electronic shopping carts typically store information in cookies that saves the state of the cart to be retrieved when the shopper visits the Web page again. However, cookies should never be used to store sensitive information as the cookies themselves are usually stored in clear text in a known location. Storing sensitive information such as unencrypted credit card information, passwords, or even personal information in a cookie is risky. It is the duty of the Web page designer to prominently display information that makes the user aware of any information stored in a cookie and the user should have the option, through good Web page design, to view the information, to remove the information, and prevent any further cookies from being written by that site. The user should not have to disable all cookies in their browser settings to prevent cookie information from being written by a single site. Many Web sites have detailed “cookie policies” that explain how they are going to use cookies. For example, Yahoo!’s cookie policy [8] includes:

- Access your information when you "sign in" so we can provide you with customized content or remember the last page you visited in a Yahoo! product or service.
- Keep track of preferences you specify while you are using Yahoo! products or services.
- Deliver advertisements relevant to your interests when you visit the branded Yahoo! network of web sites or sites in the Yahoo! advertising network outside of the branded Yahoo! network of sites, using a cookie that gathers anonymous information based on visits to Yahoo! network sites.
  - If you would rather not receive customized advertising off of the branded Yahoo! network of web sites, you can opt-out of this service.

This policy brings up many ethical questions. For example, one of Yahoo!’s services is their search engine. Cookies can be used to store tracking information, such as which Web pages you have visited, what you have typed, or even where you have moved the mouse. Finding the Yahoo! cookie policy page can be quite challenging. To get to the Yahoo! cookie policy page, you must go to the Yahoo! main page, find “Terms of Service”, written in tiny 5.5 point Verdana font at the bottom of the page, click on the link, scroll down on the next web page to YAHOO! PRIVACY POLICY, click on another link to the full privacy policy at http://info.yahoo.com/privacy/us/yahoo/. On the left side of this page, displayed in an eye-popping 9 point Arial font, under “Special Topics” is a link to Yahoo! Cookies. Clicking on this link brings you (finally!) to the Yahoo! Cookie policy. After a long and arduous journey to the Yahoo! cookie policy page you are shocked to find that Yahoo! allows for unrestricted use of Yahoo! cookies by unnamed third parties, the so-called “third-party” cookies. Their policy for third party use states [8]:

- In addition to Yahoo! using cookies, we allow certain third parties and affiliates to set and access their cookies on your computer.
- Those companies provide auditing, research and reporting for advertisers.
Advertisers' and researchers' use of cookies is subject to their own privacy policies, not the Yahoo! Privacy Policy. This is another case of hidden information. A cookie policy this liberal should be displayed in a prominent position on the main Web page or a prominent link just off the main page. Students should be taught in Web a design class that hiding this type of information on a Web site is unethical and that privacy policies in general need to be explained in a straightforward manner, they should be explained in layman’s terms, and they should always be easily accessible from the main page. In addition, all transfer and storage of information should be addressed in the policy. For educational purposes, Yahoo! provides the perfect example of what not to do.

CONCLUSIONS

It is important that topics in ethics be taught across the computing curriculum. Web design courses provide a perfect opportunity to make students more aware of ethical issues that they will face in their future careers. As the Internet continues to grow and Web technologies continue to get more sophisticated, it is important that we, as teachers, emphasize the need to apply Web technologies in a responsible manner.

REFERENCES