Cookies and Web Browser Design: Toward Realizing Informed Consent Online

Lynette I. Millett
Dept. of Computer Science
Cornell University
Upson Hall
Ithaca, NY 14853 USA
+1 202 334 3347
millett@cs.cornell.edu

Batya Friedman
The Information School
University of Washington
Box 352840
Seattle, WA 98195 USA
+1 206 616 2548
batya@u.washington.edu

Edward Felten
Dept. of Computer Science
Princeton University
35 Olden Way
Princeton, NJ 08544 USA
+1 609 258 5906
felten@cs.princeton.edu

ABSTRACT
We first provide criteria for assessing informed consent online. Then we examine how cookie technology and Web browser designs have responded to concerns about informed consent. Specifically, we document relevant design changes in Netscape Navigator and Internet Explorer over a 5-year period, starting in 1995. Our retrospective analyses leads us to conclude that while cookie technology has improved over time regarding informed consent, some startling problems remain. We specify six of these problems and offer design remedies. This work fits within the emerging field of Value-Sensitive Design.

Keywords
Informed consent, computer ethics, cookies, e-business, e-commerce, ethics, human-computer interaction, human values, interface design, Internet Explorer, locus of control, Netscape Navigator, online interactions, personalization, privacy, security, social computing, social impact, tracking, Value-Sensitive Design, Web browsers, World Wide Web.

INTRODUCTION

A cookie is a small text string (often no more than an ID number) that is sent by a Web server to a browser. The text is then stored by that browser, typically on the user's hard drive, and sent back to a Web server at a later time. Web browsers first supported cookies in 1995. They were initially developed to provide a way for users to re-visit sites without having to identify themselves and their preferences each time.

In subsequent years, however, cookies have been used in ways that substantively invade users privacy. For example, cookies have been used by third party Web sites to create user profiles without the users' knowledge, and to track users' online activities across Web sites and visits.

These and many other concerns have garnered national attention. The overarching problem can be categorized as involving informed consent: that users were neither adequately informed about what cookies do and how personal information would be used, nor adequately given a choice to decline participation.

In this paper, we first provide criteria for assessing informed consent online. Then we examine how browser designers have responded to such concerns about informed consent. Specifically, we document relevant design changes in Netscape Navigator and Internet Explorer over a 5-year period, starting in 1995. Our retrospective analyses leads us to conclude that while cookie technology has improved over time regarding informed consent, some startling problems remain. We specify six of these problems and offer design remedies.

CRITERIA FOR INFORMED CONSENT ONLINE[1]

But before we can examine how well cookies and Web browsers support informed consent, we need a better conceptual understanding of what exactly informed consent entails. Both words, "informed" and "consent", carry import [1, 3, 6]. The idea of

[1] See Friedman, Felten, and Millett [6] for a detailed discussion of the conceptual model for informed consent online that underlies these criteria.

"informed" encompasses disclosure and comprehension. In turn, the idea of consent encompasses voluntariness, comprehension, and agreement. These five components – which we will use as criteria – for informed consent online can be understood as follows:

Disclosure refers to providing accurate information about the benefits and harms that might reasonably be expected from the action under consideration. The level of description should avoid unnecessary technical detail; the information disclosed should also disabuse the individual of any commonly held false beliefs; and the reason for undertaking the action should be made explicit. Moreover, if the action involves collecting information about an individual, then the following should also be made explicit: i) what information will be collected; ii) who will have access to it; iii) how long it will be archived; iv) what it will be used for; and v) how the identity of the individual will be protected.

Comprehension refers to the individual's accurate interpretation of *what* is being disclosed. What criteria must be satisfied in order to say that something has been adequately comprehended? While there is no easy answer here, at least two methods seem viable: i) being able to restate in different words what has been disclosed, and ii) being able to apply what has been disclosed to a set of hypothetical events.

Online interactions lack the benefit of face-to-face interactions that can help ensure comprehension though dialogue. In typical Web-based interactions, users are presented with a Web page or dialog box containing disclosure information and provided with an opportunity to agree or decline to participate by clicking on a button. No queries. No talk. Special efforts on the part of Web designers will be necessary to analyze what users need to understand about a particular disclosure and to utilize strategies to increase the likelihood that comprehension will be realized.

Voluntariness refers to ensuring that the action is not controlled or coerced. Coercion is an extreme form of influence that controls by compulsion, threat, or prevention (e.g., an overt threat of violence), and thereby violates the component of voluntariness. A less obvious form of coercion can occur when there is only one reasonable way for individuals to receive certain needed services or information. This less obvious form of coercion is a serious concern for online interactions. Currently (and for the foreseeable future), sites engage in strikingly similar practices with respect to informed consent. If there is a service or information that individuals need to obtain online, then to participate in these services individuals must engage in Web interactions. Given the lack of substantive choice among Web sites and browsers, users can in effect be coerced into Web-based interactions that compel them to give up personal information or engage in other activities.

Manipulation of certain forms can also undermine voluntariness, particularly when it alters the individuals' choices or perception of choices by some means other than reason. Manipulation of the sort we are concerned with can be achieved in at least three ways: i) manipulation of the options presented to the individual such that the presentation encourages certain choices or behaviors, ii) manipulation of information, and iii) psychological manipulation. Work by Reeves and Nass and their colleagues [11, 15], for example, indicates that in online interactions individuals are vulnerable to psychological manipulation from flattery, criticism, and gender cues.

Competence refers to possessing the mental, emotional and physical capabilities needed to be capable of giving informed consent. The component of competence is used to distinguish persons from whom it is appropriate to obtain informed consent. Web designers of sites targeted for children and adolescents, for example, will need to be especially cognizant of the component of competence.

Agreement refers to a reasonably clear opportunity to accept or decline to participate. In online interactions, opportunities to accept or decline should be visible and readily accessible rather than buried under layers of menus or hidden in obscure locations.

In traditional human subjects research, the component of agreement is ongoing. Participants may withdraw their agreement to participate at any time and for any reason. While the arena of research differs in important ways from online interactions, the aspect of ongoing agreement may have relevance for online interactions. For example, users could be provided with the opportunity to withdraw their data from a recommendation system at any time. As a society, we have a good deal of experience with *implicit* consent: by virtue of entering into a situation the individual agrees to the activities that are known to occur in that context. Implicit consent holds when

the other criteria discussed above have also been met.

COOKIES AND WEB BROWSERS: A RETROSPECTIVE ANALYSIS

We are now in a position to use these five criteria – disclosure, comprehension, voluntariness, competence, and agreement -- to assess how well cookies and Web browser have supported informed consent online. We begin with a retrospective analysis of Netscape Navigator, the first browser to enable cookies. We then follow with a shorter discussion of Internet Explorer.

Methods

We independently confirmed browser preferences and default settings in Netscape Navigator (NS) versions 2, 3, 4, and 4.6 and Internet Explorer (IE) versions 3, 4, and 5. Copies of these browsers were obtained from Netscape Products: Archived Products [13], Internet Explorer Products Download [9], or available on our desktops. In addition, we obtained information about the browsers from outside documentation [2, 10, 18]. Information on browser release dates was gathered from several online sources [8, 12, 16, 19, 20].

Netscape Navigator

According to Cookie Central [2], cookies emerged in April 1995 with NS 1.1 and have existed in all later versions. In 1.1, users could not set any cookie preferences, users were not notified when a Web site wished to set a cookie, and all cookies were accepted. Four components of informed consent – *disclosure*, *comprehension*, *voluntariness*, and *agreement* – were ignored.

In version 2.0, NS began to provide some minimal limitations. According to Cookie Central, in version 2.0 each site could set no more than three cookies, each with a maximum size of 4 KB. However, in our tests with version 2.02 we were able to have the browser accept four cookies from Amazon.com. It may be that this limitation was only implemented in NS 2.0. In any case, the user still could not set cookie preferences, was not notified when a Web site wished to set a cookie, and all cookies were accepted. At that time, it was possible for sophisticated users to edit the cookie file to partially disable cookies; however doing so involved both disregarding the "do not edit" warning in the cookies.txt file (where the cookie data is stored) and modifying the file's attributes. This is not the sort of activity one would expect of typical users. From the perspective of informed consent, NS 2.0 offered little improvement over 1.1.

NS 3.0 appeared in the summer of 1996; it made significant progress in informing users about cookies and allowing the user some control. While the default setting was to "accept all cookies", for the first time users could set a preference (under Options/Network Preferences/Protocols), choosing between (a) accepting all cookies or (b) being alerted before accepting any cookie. With the alert option, each time a site requested to set a cookie, the user would be presented with a dialog box disclosing: i) what server wished to set the cookie, ii) what server could use the cookie in the future iii) the ID for the cookie, iv) the contents of the cookie (typically encrypted), and v) the cookie's expiration date. The dialog box then provided the user with an opportunity to accept or decline the cookie (see Figure 1). On the surface, version 3.0 appears to have made good progress toward realizing informed consent with respect to cookies.

However, NS 3.0 still leaves much to be desired. While a good deal of information has been *disclosed*, it is not clear that it is the right sort of information. The dialog box tells the user nothing about the expected benefits or harms from accepting this cookie, nor does it tell the user why

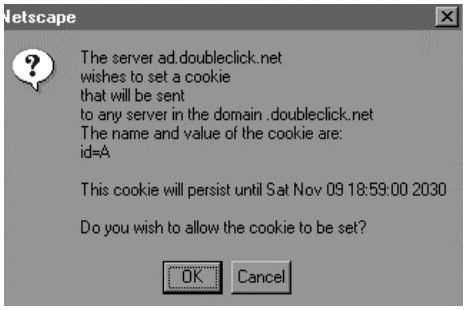

Figure 1: NS 3.04 Cookie Warning Dialog Box

the site wishes to set the cookie, what the information will be used for, or if the user's identity will be protected. To Netscape's credit, the dialog box does disclose what servers will have access to the information, indicate how long the cookie will be archived, and show the user the data that will be stored.

Even so, there will likely be a lack of *comprehension* about what is disclosed. For example, while the term "domain" has a precise technical definition, how does a typical user interpret the statement "any server in the domain 'so-and-so' "? Does that include only servers

owned and maintained by that organization? Or do users understand the term "domain" to be more broadly construed to mean servers belonging to other organizations with which the organization has a relationship? Moreover, if the cookie's value contains encrypted information, how is the user to understand it? It could be innocuous information or something quite personal; the user has no way of knowing.

Finally, in terms of *agreement*, while the opportunity to decline now exists, the implementation thrusts undue burden upon the user. While users who wish to accept every cookie can do so without doing anything, users who wish to decline every cookie must painstakingly, cookie after cookie, explicitly decline each one. In a world of Web-based interactions where cookies abound, the burden to refuse all cookies is staggering. Also, users must navigate through a cumbersome three levels of menus to locate the preference settings that allow them to decline each cookie.

Enter Netscape Navigator 4.0 roughly a year later, boasting significant improvement in the cookie preference settings (under Edit/Preferences/Advanced) available to users (see Figure 2). The options now include:

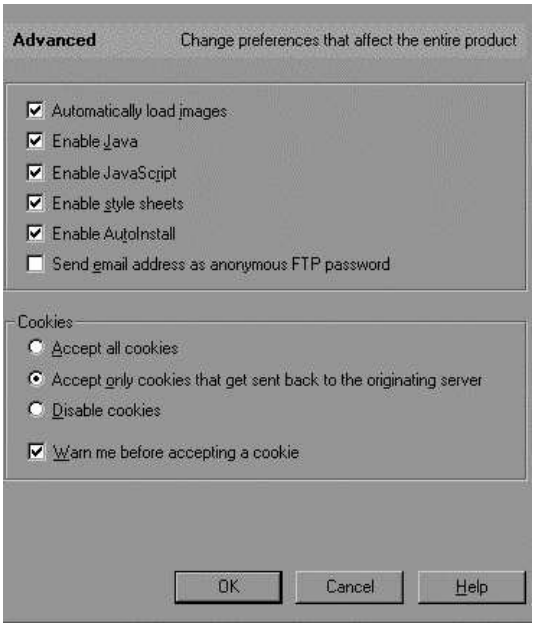

Figure 2: NS 4.03 Cookie Settings

- *Accept all cookies.* This remains the default.
- *Accept only cookies that get sent back to the originating server.* The browser will only accept cookies that are returned to the domain the user is currently connected to.
- *Disable cookies.* Decline all cookies.
- *Warn me before accepting a cookie.* When a Web site tries to set a cookie, display a dialog box that contains information about the cookie and allows the user to accept or decline. The dialog box is the same as that in NS 3.0.

From the perspective of *agreement*, NS 4.0 has eliminated the burden on the user to decline all cookies. Now declining all cookies is as simple as the decision to accept all cookies: a preference setting. In addition, another new option addresses concerns about cookies from third party sites. In the early use of cookies, users could assume that the site the user had connected to would be the site the cookie would be returned to. As cookie technology developed, third party sites began to make use of cookies, typically through the use of banner ads but also through the use of one-pixel images, effectively invisible to the user. Thus, users could no longer assume that a cookie apparently being sent from the visited site would be returned to that site. Moreover, these third party cookies were often used for targeted marketing purposes and to track the user's visits among various sites. With the new option, users could set a preference that allowed them to easily agree to all cookies that would be returned to the site the user was currently visiting but decline all those that would be returned to third party sites. Finally, we note that despite these new options, the "accept all cookies" option is still privileged as the default setting. When the user installs and launches Netscape Navigator 4.0, cookies are enabled and the browser will never inform the user about their use.

A few words also need to be said about the component of *comprehension*. The option "accept only cookies that get sent back to the originating server" is likely to elicit the response "What does that mean?" from the typical user. The less technically precise phrase, "decline all cookies from third party Web sites" might match more closely the users' understanding. To better ensure comprehension of this option, some amount of user testing will be required. In addition, the preference menu allows users to choose one of the first three options AND whether or not to be warned before accepting a cookie. In some cases it is unclear what these combinations might mean. For example, if a user selects "accept all cookies" and "warn me before accepting a cookie" will the browser accept all cookies automatically and tell

BROWSER	Netscape Navigator					Internet Explorer		
Version	1.1	2.02	3.04	4.03	4.6	3.0	4.0	5.0
Release Date (typically of the X.0 version).	4/95	3/96	8/96	6/97	5/99	8/96	8/97	3/99
Where cookies are stored on the user's machine.	?	1 file	1 file	1 file per user	1 file per user	Multiple files	Multiple files	Multiple files
Limitations on the number and size of cookies.	?	Yes	<300	<300	<300	User sets	2% of hard drive or user sets	2% of hard drive or user sets
Number of menu levels to set cookie preferences.	N/A (no pref. set.)	N/A (no pref. set.)	3	3	3	*3	3	3 or 4
PREFERENCE "Accept all/None" option available.	No	*No	No	Yes	Yes	No	Yes	Yes
PREFERENCE "Obtain consent before accepting" option available.	No	No	Yes	Yes	Yes	Yes	Yes	Yes
PREFERENCE "Accept some/All/None" option available.	No	*No	No	Yes	Yes	No	No	Yes
DEFAULT SETTING Initial setting.	Accept all cookies (cannot be altered)	Accept all cookies	Accept all cookies	*Accept all cookies	Accept all cookies	*Accept all cookies	*Accept all cookies	Accept all cookies (Internet Zone = medium)

Table 1
Summary of Browser Cookie Features by Browser and Version Number
* = Unable to verify independently, assumption based on previous and subsequent browser version capabilities. ? = Unable to obtain this data.

the user it has done so each time? Or will the browser warn the user about each cookie and allow the user to agree or decline? Accurate interpretations on the part of the user will require a less ambiguous interface.

In terms of *disclosure*, the option "disable cookies" might be better phrased as "decline all cookies", and the option "warn me before accepting a cookie" might be better phrased as "obtain my permission before accepting a cookie". These recommended wording changes help clarify the user's role in providing agreement and replace words with potentially negative connotations ("disable", "warn") that might dissuade unsophisticated users from choosing these options with less emotion-laden terms.

Nearly two years later, in 1999 – two years during which cookies gained increasing visibility in the media and privacy appears foremost in users' concerns about Web use – version 4.6 appears. Surprisingly, with respect to cookies, NS 4.6 provides no significant changes from version 4.0.

Internet Explorer

As shown in Table 1, Internet Explorer follows a similar evolution regarding cookies and informed consent. In brief: IE 3.0 shares many key features with its contemporary NS 3.0. Both browsers i) provided a single cookie preference setting, "warn

before accepting cookies" that placed the burden for declining all cookies on the user, ii) accepted all cookies as the default, and iii) provided roughly comparable information about the cookie in the warning dialog box. Notably, the IE 3.0 warning box does not tell the user where the cookie may be returned to, thus, there is no way to distinguish third party cookies.

IE 4.0 offers improvements over IE 3.0 but lags somewhat behind its contemporary NS 4.0. In terms of cookie preference settings, IE 4.0 now allows the user to "disable all cookie use", however, unlike with NS 4.0 the user must still recognize and decline third party cookies on a case-by-case basis. IE 4.0 has also changed the format of its cookie warning dialog box and users must now click an additional (unnecessary) button to obtain detailed information about the cookie. Information about the cookie's name and its security status (though it is unclear what this means) is now provided (see Figure 3).

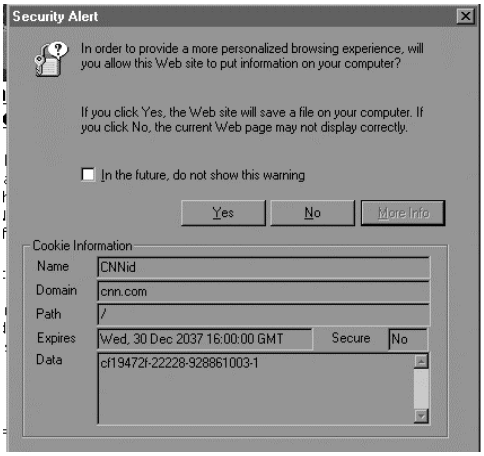

Figure 3: IE 4.0 Cookie Warning Dialog Box

IE 5.0, appearing in 1999 and contemporary with NS 4.6, reconceptualized the IE interface for determining cookie preferences. A two-tiered system was put in place. In the first tier, the user selects a security level (found at Tools/Internet Options/Security) that determines a constellation of preference settings as a whole. Of the four possible security levels, only the "High" level reveals its default cookie setting: "cookies are disabled"; the other levels "Medium", "Medium-Low", and "Low" make no mention of cookies. Moreover (and as revealed elsewhere in the browser), at these three lower security levels the default settings are set to accept all cookies.

Users can also choose to customize the constellation of preference settings associated with each security level by clicking the "Custom Level" button. In this second tier, users discover that preferences for cookies that are stored on the user's computer have been separated from cookies that exist only for the duration of the session. In addition, the options have been renamed to "disable", "enable", and "prompt", which removes the negative connotations associated with warnings (see Figure 4). Note, however, there is still no option to decline all third party cookies.

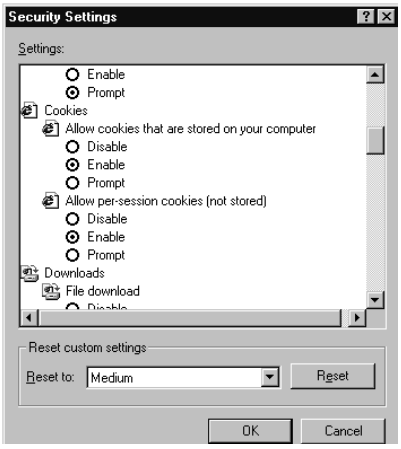

Figure 4: IE 5.0 Custom Cookie Settings

DESIGN REMEDIES

It is now five years since cookies were first enabled without any support from the browser for realizing informed consent. During this time, some progress has been made in what is disclosed to users, the comprehensibility of the language that is used, and the options with which users can agree to or decline the use of cookies.

Still, some startling problems remain. In the section that follows, we highlight five of these problems and offer remedies.

- *The information disclosed about a cookie still does not adequately specify what the information will be used for or how the user might benefit or be harmed by its use.*

Remedy: Redesign the browser's cookie dialog box to include three additional fields, one for stating the purpose for setting the cookie, one for a brief statement of benefits, and one for a brief statement of risks. The presence of these fields would encourage sites to disclose this information to users. That said, the content of these fields will remain under the control of each site and users will need to rely on the honesty thereof.

- *In order to change cookie preference settings to something other than "accept all cookies", a user needs to traverse a minimum of three menu levels to locate the preference settings.*

Remedy: Cookie preferences should be located in a meaningful menu hierarchy – perhaps under a menu labeled something like "Privacy and Security Settings" – and as close to the top of the hierarchy as possible.

- *In Internet Explorer, the burden to decline all third party cookies still falls to the user who must decline each cookie one at a time.*

Remedy: Redesign the browser preference setting to include a comprehensibly-labeled option to decline all cookies that would be returned to third party Web sites.

- *None of the browsers provide the user with control over how long a cookie will exist on the user's machine.*

Remedy: Redesign the browser to allow users to easily delete a cookie or to change a cookie's expiration date.

- *The default cookie setting for current browsers was "accept all cookies." Thus, novice users' "out-of-the-box" experience of cookies for NS 4.6 or IE 5.0 in mid-1999 was no different than their "out-of-the-box" experience of cookies for NS 1.1 in 1995.*

Remedy: What is needed here is a default that preserves informed consent without unnecessarily burdening the user with overwhelming and potentially nonsensical queries. For sophisticated users, the default setting to prompt the user about each cookie would protect informed consent without too great a burden. For novice users, a default setting to "decline all cookies" would, under the right conditions, preserve the novice user's informed consent and eliminate the overwhelming presentation of cookie warning messages. But the right conditions would mean that many Web sites must be redesigned to allow users who decline cookies to navigate the sites effectively (albeit without personalization). We come back to this point shortly.

Lastly, we call attention to a sixth problem for which we see no easy remedy. The problem is this:

- *No browser alerts a user to when a site wishes to use a cookie, as opposed to store a cookie.*

A user may be comfortable with one use of a cookie but not with another use of the same cookie. However, currently users have no way to "agree" to the particular use but only to the setting of the cookie in the first place. The source of this problem lies in the interaction between the browser design and corresponding Web site expectations as follows: Upon initiating a connection with a remote site, the Web browser automatically offers the Web site its cookie file if the Web site has a cookie stored in that file. Thus, in practice, the Web site never actively requests a cookie. True, a redesigned standard could allow the Web browser to initiate a connection to a Web site without automatically offering the cookie file. And if that were the case, whenever a Web site wished to look at a cookie, the site would need to actively request the cookie file from the Web browser. However, such a redesign on the part of the browser would require a corresponding and comprehensive redesign on the part of *all* Web sites and, therein, lies the difficulty of the remedy. In hindsight, we observe that browsers (and other software) should not be designed to volunteer information without putting in place some override mechanism.

CONCLUSION

Since 1995, the industry has made a sustained effort to realize informed consent for cookie technology. Progress has been made with respect to disclosure, comprehension, and agreement. Yet, as demonstrated by our analysis, substantive problems remain. Some of these problems can be easily remedied, and we have specified how. For example, Web browsers should be redesigned to allow users to easily delete a cookie and to change a cookie's expiration date. Another example: the browser preference setting on Internet Explorer should be redesigned to include a comprehensibly-labeled option to decline all cookies that would be returned to third party Web sites.

Other of our remedies are difficult to implement because changes must occur at levels no longer within reach of the browser itself. For example, as we mentioned above, in fostering usability and informed consent, novice users would be best served if the default condition declined all cookies – but only if Web sites allowed novice users to navigate their sites without impediment. But currently that condition is not met. Thus unfortunately novice users must now give ground on informed consent to achieve usability.

Of course, had browsers in 1995 (or even in 1997) implemented "decline all cookies" as the default setting, sites seeking to attract novice users (i.e., most sites) would have responded with designs that were functional without cookies. In other words,

the best remedies may no longer be possible because we are several years too late in noticing the problems and taking action.

Thus our two larger ideas become apparent. First, with regard to many human values – such as informed consent, but also including trust, autonomy, freedom from bias, accountability, privacy, and universal access – it is much easier to design proactively to protect and foster these values than it is to retrofit existing designs. This idea fits within the emerging field of Value-Sensitive Design [4, 5, 7, 14, 17].

Second, it is all too common in quickly changing technological fields for the pace (and demands) of development to trump any historical considerations of how and why designs have emerged as they have. Young designers in particular, we fear, have a "technological amnesia" -- where 2 months is considered old, and 2 years irrelevant. It is our hope that retrospective analyses, such as provided in this paper, quicken interest in the not-so-distant past so that we can design better for the not-so-distant future.

ACKNOWLEDGMENTS

This paper is accepted for presentation at CHI 2001 and will appear in the *CHI 2001 Proceedings*. This research was funded by the National Science Foundation Award IIS-9911185. We thank Peter H. Kahn, Jr. for his comments on earlier versions of the manuscript.

REFERENCES

1. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1978.
2. Cookie Central. All copyright 1997, 1998, Cookie Central. http://www.cookiecentral.com .
3. Faden, R, and Beauchamp, T. *A History and Theory of Informed Consent*. Oxford University Press, New York NY, 1986.
4. Friedman, B. (Ed.) *Human Values and the Design of Computer Technology*. Cambridge University Press, New York NY, 1997.
5. Friedman, B. Value-Sensitive Design: A Research Agenda for Information Technology. (Contract No: SBR-9729633). National Science Foundation, Arlington, VA, 1999.
6. Friedman, B., Felten, E., and Millett, L. I. *Informed Consent Online: A Conceptual Model and Design Principles*. UW-CSE Technical Report Number 2000-12-2, 2000.
7. Friedman, B., Kahn, P. H., Jr., & Howe, D. C. Trust online. *Communications of the ACM*, 43(12), (2000), 34-40.
8. "IE5 release data announced as March 18th, 1999." Thread in uk.comp.os.win95.
9. *Internet Explorer Products Download*. http://www.microsoft.com/windows/ie/download/ie5all.htm .
10. Mayer-Schonberg, V. The Internet and privacy legislation: Cookies for a treat? *West Virginia Journal of Law and Technology 1(1),* 1997. http://www.wvjolt.wvu.edu/wvjolt/current/issues1/articles/mayer/mayer.htm .
11. Nass, C. I., Moon, Y., Morkes, J., Kim, E., & Fogg, B. J. Computers are social actors: A review of current research. In B. Friedman (ed.), *Human Values and the Design of Computer Technology* (pp. 137-162). Cambridge University Press, New York NY, 1997.
12. "Netscape 4.6 is out…" Thread in visi.general.
13. *Netscape Products: Archived Products*. http://home.netscape.com/download/archive/index.html .
14. Nissenbaum, H. Accountability in a computerized society. *Science and Engineering Ethics, 2* (1996), 25-42.
15. Reeves, B., & Nass, C. *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places.* Cambridge University Press, New York NY, 1996.
16. "Relese [sic] date for NSC4?" Thread in comp.infosystems.www.browsers.ms-windows.
17. Thomas, J. C. Steps toward universal access in a communications company. In B. Friedman (ed.), *Human Values and the Design of Computer Technology* (1997), Cambridge University Press, New York NY, 271-287.
18. Whalen, D. *The Unofficial Cookie FAQ V. 2.53*. http://www.cookiecentral.com/faq/. May, 1999.
19. Wilson, B. *Browser History, Internet Explorer*. http://kempelen.inf.bme.hu/htmlhelp/history/ie.htm
20. Wilson, B. *Browser History, Netscape.* http://kempelen.inf.bme.hu/htmlhelp/history/netscape.htm