Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design

Batya Friedman and Daniel C. Howe
The Information School
University of Washington
batya@u.washington.edu
dchowe@u.washington.edu

Edward Felten
Department of Computer Science
Princeton University
felten@cs.princeton.edu

Abstract

This paper reports on one of the first efforts to apply Value-Sensitive Design (VSD) to a large-scale real-world software system. We sought to improve informed consent in Web-based interactions through the development of new technical mechanisms for cookie management. We describe our VSD methodology, explicate criteria for informed consent in online interactions, and summarize how current browsers fall short with respect to those criteria. Next we identify four goals for the redesign of current browsers. These goals, in turn, initiate an iterative design process that lies at the heart of the VSD methodology – wherein we move among the design and implementation of new technical mechanisms, formative evaluation, and the design goals coupled with the criteria for informed consent online. Key mechanisms include: peripheral awareness of cookies, and just-in-time interventions. At various phases in the design process, we implement our design improvements in the Mozilla browser (the open-source for Netscape Navigator).

1. Introduction

Informed consent provides a critical protection for privacy, and supports other human values such as autonomy and trust. Yet currently there is a mismatch between industry practice and the public's interest. According to a recent report from the Federal Trade Commission [8], for example, 59% of Web sites that collect personal identifying information neither inform Internet users that they are collecting such information nor seek the user's consent. Yet, according to a Harris poll [18], 88% of users want sites to garner their consent in such situations. The Federal Trade Commission [8, p. iv] hopes that industry will continue to make progress on this problem, in conjunction with its proposed legislation. Toward such progress, however, we in the computing community should be helping to shape the dialogue by providing technical means to realize informed consent in online interactions.

This paper reports on our effort to improve support for informed consent in Web-based interactions, particularly through the development of new technical mechanisms for cookie management in the Web browser. We chose to focus on the browser because browsers play a critical role in informing the user about a Web site's desire to set a cookie and in determining how the cookie will be handled on the users' machine. Drawing on our prior work, we first describe criteria for informed consent in online interactions [14] and, in light of those criteria, summarize how current browsers fall short [27]. Next we identify four goals for the redesign of current browsers to improve support for informed consent. These four goals, in turn, initiate an iterative design process that lies at the heart of the Value-Sensitive Design methodology – wherein we move among the design and implementation of new technical mechanisms, formative evaluation, and the four design goals coupled with the criteria for informed consent online. At various phases in the design process, we implement our design improvements in the large-scale real-world open-source browser Mozilla (the open-source for Netscape Navigator). Thus, our end product is integrated into an existing browser and can be made available to the public.

In addition to the new technical mechanisms we report here, this work represents one of the first efforts to apply a Value-Sensitive Design approach to a large-scale real-world software system. In brief, Value-Sensitive Design is an approach to the design and implementation of systems that systematically and comprehensively accounts for human values throughout the design and implementation process [9, 10, 11, 13]. In Value-Sensitive design conceptual, technical, and empirical investigations are employed iteratively throughout the design and implementation process. C*onceptual* investigations provide philosophically informed analyses of the central constructs and issues relevant to the system under development. T*echnical* investigations identify

0-7695-1435-9/02 $17.00 (c) 2002 IEEE

how existing technical designs and mechanisms engender value suitabilities and, conversely, how the identification of specific values can lead to new technical designs and mechanisms to support better those values. E*mpirical* investigations draw on social science methodologies to understand the value-oriented perceptions and experiences of the direct and indirect stakeholders of a given system. The Value-Sensitive Design investigations are employed in consort with other already successful technical methods [1, 5, 13, 15, 21].

In addition to Value-Sensitive Design, four other central approaches to human values, ethics, and design can be identified [12]. These approaches include Computer Ethics that has focused on how to utilize existing moral theory to bring clarity to ethical issues involving computer technology and, conversely, on how such technological innovations extend the boundaries of traditional ethical concepts [23, 28, 32]. The second approach is Social Informatics that emphasizes socio-technical analyses of deployed technologies that take into account their interaction with institutional and cultural contexts [4, 20, 25, 31]. The third approach is Computer Supported Cooperative Work (CSCW) that has focused on the design of new technologies to help people collaborate effectively in the workplace. The values considered in CSCW designs have been closely tied to group activities and workplace issues [16, 19, 22, 30]. The fourth approach is Participatory Design that fundamentally seeks to integrate worker's knowledge and a sense of work practice into the system design process. Traditionally, Participatory Design has embedded within it a commitment to democratization of the workplace and human welfare [3, 17, 26].

Researchers are just now beginning to apply Value-Sensitive Design methodologies proactively in the design process. Thus our work contributes not only to specific knowledge on how to support informed consent in Web-browser design and the redesign of the open-source Mozilla browser, but explicates and extends the systematic use of Value-Sensitive Design methodologies in the context of large-scale real-world software systems.

2. Criteria for informed consent online

Before we can design cookie and Web browser technologies to support informed consent, we need a robust conceptual understanding of what exactly informed consent entails. Both words, "informed" and "consent", carry import [7, 14, 2].

The idea of "informed" encompasses disclosure and comprehension. *Disclosure* refers to providing accurate information about the benefits and harms that might reasonably be expected from the action under consideration. *Comprehension* refers to the individual's accurate interpretation of *what* is being disclosed. In turn, the idea of "consent" encompasses voluntariness, comprehension, and agreement. *Voluntariness* refers to ensuring that the action is not controlled or coerced. *Competence* refers to possessing the mental, emotional and physical capabilities needed to be capable of giving informed consent. *Agreement* refers to a reasonably clear opportunity to accept or decline to participate. Moreover, the component of agreement is ongoing. See [14] for an expanded discussion of these five criteria.

In addition, the empirical investigations conducted as a part of this research yielded a sixth criterion, that of minimal distraction. *Minimal Distraction* refers to meeting the above criteria without unduly diverting the individual from the task at hand. Minimizing distraction is an inherent challenge for any implementation of informed consent as the very process of informing users and obtaining their consent necessarily diverts users from their primary task. Two sorts of situations are of concern here. First, if users are overwhelmed with queries to consent to participate in events with minor benefits and risks, they may become numbed to the informed consent process by the time participation in an event with significant benefits and risks is at hand. Thus, the user's participation in that event may not receive the careful attention that is warranted. Alternatively, if the overall distraction to obtain informed consent becomes so great as to be perceived to be an intolerable nuisance, users are likely to disengage from the informed consent process in its entirety and accept or decline participation by rote. Thus undue distraction can single-handedly undermine informed consent.

3. Retrospective analysis of cookies, browsers, and informed consent

With criteria for assessing informed consent in hand, we next conducted a retrospective analysis of existing browser technologies to identify where they fall short with respect to informed consent [27]. Specifically, we documented how design changes in Netscape Navigator and Internet Explorer from 1995 - 1999 responded to concerns about informed consent. From the perspective of Value-Sensitive Design methodology, the retrospective analysis represents a technical investigation that is informed by the results of a prior conceptual investigation.

In brief, through the retrospective analysis we found that while cookie technology has improved over time regarding informed consent (e.g., increased visibility of cookies, increased options for accepting or declining cookies, access to information about cookie content), some startling problems remain. For purposes of this paper, we summarize key results here:

- While browsers now disclose to users some information about cookies, they do not disclose

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

the right sort of information - that is, information about the potential harms and benefits from setting a particular cookie.

- Through preference settings, browsers now offer users many more options for managing cookies. But these preference settings are typically located in obscure menu hierarchies and pose challenges for opportunities to accept or decline participation.
- In Internet Explorer, the burden to accept or decline all third party cookies still falls to the user, placing undue burden on the user to decline each third party cookie one at a time.
- As of 1999, browsers provided users with no means to control how long a cookie would remain on the user's machine. (Note: In January 2000, Netscape Navigator added the feature to 'delete' a cookie that partially remedies this situation.)
- Users' 'out-of-the-box' experience of cookies (the default setting) is no different in 1999 than it was in 1995: to accept all cookies. That is, the novice user installs a browser that accepts all cookies and discloses nothing about that activity to the user.
- No browser alerts a user to when a site wishes to use a cookie and for what purposes, as opposed to when a site wishes to store a cookie.

4. Four overarching design goals

From our retrospective analysis of cookies, current browsers, and criteria for informed consent, four primary goals emerged as central to our redesign effort. We discuss each goal in turn.

Design Goal 1: Enhance users' local understanding of discrete cookie events as the events occur with minimal distraction to the user. Current browsers require users to select a preset agreement policy that applies to all cookies of a specified type (e.g., accept all cookies; decline all third party cookies) or to explicitly accept or decline each cookie one at a time. The former mechanism– presetting a general policy – minimizes user distraction at the expense of rote decision-making, disclosure and comprehension. With this type of mechanism, the user is never notified that a cookie meeting the policy has been accepted and placed on the user's machine; nor does the user have an opportunity to examine the cookie. In contrast, the latter mechanism – to explicitly accept or decline each cookie -- supports the criterion of disclosure but at the expense of extreme distraction. A middle ground is warranted here – one that provides users with some awareness of a cookie when it is set followed by the opportunity to make a decision about that cookie based on this newly acquired information but without undue distraction.

Design Goal 2: Enhance users' global understanding of the common uses of cookie technology including potential benefits and risks associated with those uses. The potential benefits and risks from accepting or declining an individual cookie is part of a larger socio-technical practice wherein cookies are used to create profiles of users over time and across sites. For users to be able to make informed choices about individual cookies, they must also possess some understanding of how an individual cookie fits into this larger socio-technical practice, including commonly employed uses of cookie technology as well as potential benefits and risks associated with such uses. For example, if a user does not understand the common practices of sites that employ cookie technologies and the implications of these technologies then disclosing the data associated with individual cookies (e.g., domain, expiration, name, value, path) will be of limited use in fostering comprehension, without which there cannot be genuine informed consent. In this way, global understanding of cookie technology is a necessary piece of disclosure and comprehension.

Design Goal 3: Enhance users' ability to manage cookies. Our retrospective browser analysis also revealed inadequate mechanisms for effective cookie management, particularly with respect to the easy viewing of cookie information and on-going control over the lifetime and removal of cookies. Specifically, with browser technology as of December 1999, users were unable to easily give and later revoke agreement for a cookie[1]. To highlight the importance of this functionality for informed consent, consider the following scenario in which a user, after reading a Web site's privacy policy, has agreed to allow a number of cookies from that site that persist between visits to be set on the user's machine. However, before the user's next visit, new owners purchase the Web site and substantively modify the site's stated privacy policies. With the 1999 browser technology, the user has no easy means to remove the previously set cookies and thereby revoke consent. Recall that in our model for informed consent, agreement is on-going - that is, users must be able to give their consent not only at the start of the interaction (as current browsers with this preference provide) but to revoke that consent at any point later in the interaction. Thus, the cookie management of 1999 technology violated the informed consent criterion of *agreement*.

Design Goal 4: Achieve design goals 1, 2 and 3 while minimizing distraction for the user. As noted earlier, the very process of informing a user and obtaining consent diverts the user from the primary task at hand. Moreover, functionality that overwhelms the user with interruptions or consumes excessive user resources will not be utilized

[1] Technically skilled users could delete cookies directly from their cookie files. However such activity required significant technical knowledge and diverted users from their primary Web-based tasks. Thus, this option was not available to users with typical skill levels and violated the criterion of *minimal distraction* for highly skilled users.

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

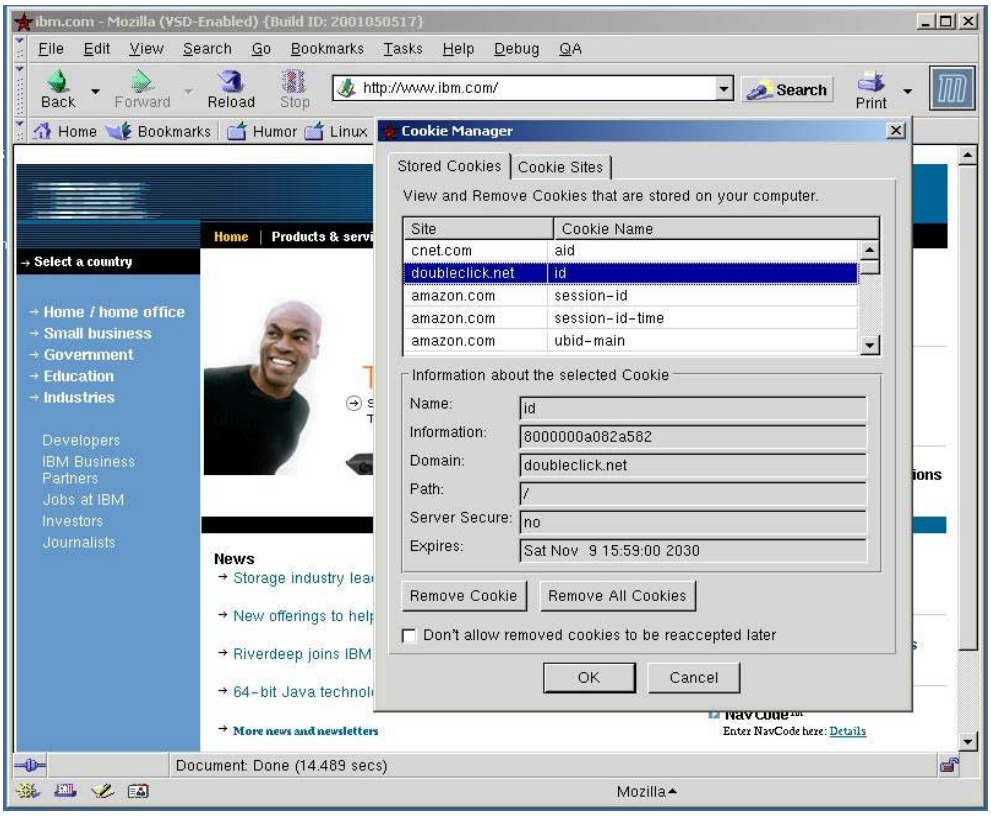

Figure 1. The Gedanken prototype (screen shot of the Cookie-Manager tool in Mozilla 0.8)

and might as well not exist. Thus, effective informed consent requires supporting mechanisms with minimal overhead for the user.

5. Prototype one: The Gedanken prototype

5.1 Description

After articulating our primary design goals of enhanced local understanding, global understanding, and cookie management with minimal distraction for the user, we began our development work with what we refer to as a *Gedanken* prototype: an initial, "imagined" design with which to begin the iterative design process. A Gedanken or thought prototype has the advantage (along with traditional cardboard mock- ups [6]) of allowing for initial design work without devoting costly resources to rapidly developing 'throw-away' UI's with RAD tools like Director or Visual Basic.

The starting point for our Gedanken prototype was Mozilla version 0.8 (see Figure 1).

Our first step involved the identification of concrete mechanisms that could potentially further the four design goals. Two key insights emerged. One entailed the potential use of *peripheral awareness* (c.f. [33]) as a strategy to increase users' awareness of cookies events as they occur without requiring direct attention from the user. Traditionally, peripheral awareness mechanisms have been used successfully to provide users with on-going information about machine state through non-attention grabbing visual or auditory cues that users may or may not choose to attend to. The second insight entailed the potential use of *just-in-time interventions* as a strategy to provide users with access to information and cookie management facilities for cookie events as they occur, while allowing for but not requiring an intervention from the user. Again, traditionally, just-in-time interventions have been used successfully to present users only with relevant information and facilities, and only at the moment when such information or facilities are *necessary* for the completion of a task or the making of a decision. Taken together, these two strategies address both the criterion of minimal distraction as well as the problem of information overload experienced by many users. In the context of the Gedanken prototype, we used the insights of peripheral awareness and just-in-time interventions to envision features (new technical mechanisms) that would:

- Make users aware of discrete cookie-events as they occur, perhaps through visual or auditory peripheral cues.

- Make users aware of different types of cookie events (e.g., third party cookie, duration of cookie) as they occur, perhaps through additional visual or auditory peripheral cues.
- Allow users to obtain detailed information about the most recently set cookie, perhaps with a just-in-time intervention that provides the user with access to the cookie's data fields and the existing Mozilla Cookie-Manager tool.
- Allow users to edit the expiration date or delete cookies separately or in groups with a just-in-time intervention that provides the user with access to the Mozilla Cookie-Manager tool.

5.2. Formative Evaluation

To identify the strengths and weakness of the Gedanken prototype at this preliminary stage, we employed a modified informal heuristic evaluation [29] that coupled traditional usability concerns (e.g., of consistency, ease-of-use) with value-oriented concerns (e.g., of disclosure, comprehension, minimal distraction, enhanced local discrete understanding of cookies, enhanced global understanding of cookies). Five graduate students in The Information School at the University of Washington were invited to conduct the informal heuristic evaluations. Each evaluator was shown a color mockup of Mozilla version 0.8 with the Mozilla Cookie-Manager window open (similar to Figure 1 above). In addition to the color mockup, we described the use of visual and auditory cues to notify users of cookie events as they occurred as well as mechanisms for allowing users to view relevant data fields of the most recently set cookie in the Mozilla Cookie-Manager by activating a button or key combination. With each evaluator, we solicited spontaneous comments on the interface itself as well as the elements of peripheral functionality not easily viewed via the paper mock-up. If evaluators did not spontaneously comment on the Cookie-Manager, we explicitly solicited feedback on the tool's functionality and interface. We attended to comments on traditional usability as well as value-oriented aspects of the prototype.

The informal heuristic evaluations yielded a good deal of valuable information about our specific design goals and the interface as a whole. Feedback from evaluators specifically identified the need for:

- An easy means to learn more about discrete cookie-events as they occurred.
- A more intuitive representation for our cookie classification scheme.
- A mechanism to permanently block a site from setting cookies, once a user had manually removed a cookie from that site (for instance, a third-party ad service).
- A mechanism to link a discrete cookie event (as indicated peripherally) with cookies identified in the Cookie-Manager.

In addition to feedback from the evaluators, our design team recognized that although our prototype presented a wide range of information about each discrete cookie stored on a user's machine in an intuitive and easy to manage fashion, there was still no way for users to conceptually link these discrete cookies with a global understanding of common practices, usage patterns, benefits, and risks associated with individual cookies.

6. Prototype two: the Mozilla Cookie-Watcher

6.1. Description

In conjunction with our criteria for informed consent online, the formative evaluation of the Gedanken prototype provided us with new data with which to return to our overarching design goals of enhanced local understanding, global understanding, and cookie management with minimal distraction for the user. Our question now was: Within the structure of the current Mozilla browser, how best can we make discrete cookie-event information available to users in a consistent fashion that would divert users' attention only at appropriate times?

We approached this question first in terms of a peripheral awareness mechanism. A robust peripheral awareness mechanism would need to notify users not only about the occurrence of a cookie-event but also about the type of cookie being set. We next considered several venues of notification: static visual notifications, flashing animation notifications, and audio notifications. Based on the heuristic evaluations and further discussion among the design team, we settled on a primarily visual notification venue – one that would take up a small but persistent area of the screen. Key justifications for this decision included the ability to link visual cues for discrete cookie events with the existing Cookie-Management toolkit, the opportunity to present persistent data about recently set cookies, and the ease with which a focused user could ignore a small visual representation on the screen. In addition, we suspected a visually-based notification system would provide far greater flexibility and expandability for representing the cookie classification scheme as it evolved, as well as custom display cues should they be desired.

With these and other design imperatives in mind, we implemented a small application – the Cookie-Watcher tool -- docked in Mozilla's sidebar window (see Figure 2). In the Cookie-Watcher, cookies appear in real-time as they are delivered to the machine. In addition, the

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

Cookie-Watcher provided classification information for each cookie according to domain and expiration that was keyed to the background color for each cookie as follows: third-party cookies (those set by other sites than the one being visited) were displayed with a red background; cookies with expirations set more than one year in the future were displayed with a yellow background; and all other cookies were displayed with a green background.

Having designed a peripheral awareness mechanism, we turned next to consider mechanisms to support just-in-time interventions. Two sorts of just-in-time interventions at the time of decision-making seemed needed: one to provide general information about cookies – the Cookie-Information Dialog Box (see Figure 2) – and one to provide access to the existing Cookie-Manager tool. Less clear was when to provide each type of just-in-time mechanism. We faced a common problem: That it is difficult, if not impossible, to know when a particular decision is in fact important to a given user in a given context. Traditionally, strategies that attempt to infer this information from users' behavior have failed as the interpretation of human behavior eludes our current knowledge and the capacity of today's computational systems. In our design, we took a somewhat different approach: we assumed that only the users themselves will be able to properly discern when their present task is one that may be disturbed and would constitute a valid disturbance of that task. In this way, the application need only make the user peripherally aware of a potential task-disrupting decision, at which time the user (perhaps even subconsciously) may opt to engage in a task-disrupting decision or to continue on with the primary task.

Having determined how users would access the just-in-time interventions, we next turned to defining each mechanism. To obtain just-in-time information about cookies in general, users could click on a button labeled "Learn More" at the bottom of the Cookie-Watcher window. At that time, the Cookie-Information Dialog Box would appear containing a text description on the nature and implications of cookies in the larger context of day-to-day usage. In our first version of the text, the discussion was brief (limited to four short paragraphs): a one-sentence definition of a cookie, a paragraph mentioning the benefits of cookies for personalization, a paragraph mentioning potential limitations and risks from cookie use, and a paragraph highlighting our modifications to the Mozilla browser. No information was provided about the color-coding in the Cookie-Watcher and no discussion was provided of the importance of domain and expiration of cookies for

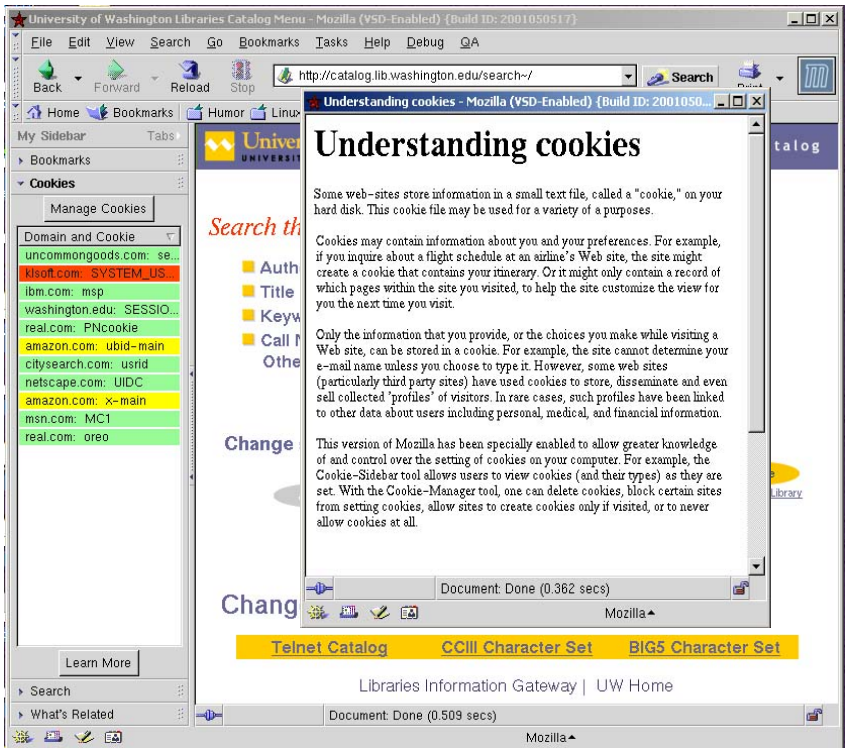

Figure 2. The Mozilla Cookie-Watcher prototype implemented in Mozilla showing the Cookie-Watcher tool (at the left) and the Cookie-Information Dialog Box (in the center).

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

assessing their potential benefits or risks. The second just-in-time intervention provided a mechanism for moving smoothly from awareness of a cookie-event to proactive cookie management. As identified in the formative evaluation, users felt the need to move from their awareness of a cookie-event directly and efficiently to more in-depth information about the particular cookie if they felt inclined to act upon it. To satisfy this requirement, we activated each line in the Cookie-Watcher so that a mouse-click would bring up the Cookie-Manager tool with the selected cookie highlighted and its data fields visible. This design change served not only to allow users to move quickly and easily from observation to management, but also helped users to construct at least some of the global understanding we had identified as an overarching design goal.

6.2. Formative Evaluation

As with our earlier formative evaluation of the Gedanken prototype, the usability study we conducted with the Mozilla Cookie-Watcher prototype were two pronged. One dimension focused on those aspects of the prototype that directly impacted the values targeted by our design efforts – in this case, informed consent. In this context, we were specifically interested in assessing how well the prototype met our theory-driven goals to enhance local understanding, global understanding, and cookie management with minimal distraction for the user. The second dimension focused on how well the interface met traditional human-computer interaction criteria, such as intuitiveness, consistency, and ease-of-use (cf. [24, 29]).

6.2.1. Participants. A formal usability study of the prototype was conducted with 8 individuals (3 male, 5 female) between the ages of 20-30. Participants were undergraduate students, graduate students, or post-graduate student employees at the University of Washington. All participants were experienced Web users (ranging from 3- 8 years of Web use) and regularly used one of the two most popular browsers, Internet Explorer 5.x and Netscape Navigator/Communicator 4.x. In pre-session interviews, two participants (25%) were significantly confused about the nature of cookies.

6.2.2. Methods. The usability study began with a pre-session semi-structured interview about participants' prior Web experience and knowledge of cookies. The pre-session interview was followed by a 30-minute hands-on session during which participants interacted with the Mozilla Cookie-Watcher prototype and completed a set of directed and non-directed Web-based browsing. During the hands-on session, participants were asked to talk aloud and machine-recorded interaction data was collected. The direct browsing ensured that all participants would encounter a wide variety of cookie interactions, including sites that used cookies for state-management, internal profiling, anonymous recommendation systems, and for featured banner ads in which third-party servers set cookies on the user's machine. The non-directed Web browsing allowed us to observe participants' use of the Cookie-Watcher in the context of their more typical browsing behavior. The hands-on session concluded with a semi-structured interview about participants' reactions to the Mozilla Cookie Watcher prototype including their assessment of the Cookie Watcher, increased awareness of information for individual cookies, increased awareness of patterns of cookie behavior, and level of distraction to attend to the cookie features. Finally, following the post-session interview and if the participant had not spontaneously interacted with the Cookie-Management tool during the directed and non-directed Web browsing, the participant was asked to perform an additional task that explicitly used the Cookie Manager tool and to evaluate that tool.

6.2.3. Results and Discussion. The majority of participants used the Cookie-Watcher spontaneously. Based on the machine-collected interaction data, five participants (63%) explored the Cookie-Watcher tool on their own. Of the three participants who did not explore the Cookie-Watcher, two stated a desire to close the tool at some point during the session in order to free up screen space on the 19" high-resolution monitor. Interestingly, these two participants were the same individuals who possessed limited or mistaken understanding of cookies in the pre-session interview.

Participants appeared to increase their awareness and understanding of cookies in a local context. In both solicited and unsolicited comments, users commented on their ability to easily recognize individual cookie-events as they occurred in real-time. Moreover, observation of participant behavior (e.g., surprise at seeing a cookie-event recorded in the Cookie-Watcher) confirmed participants' recognition of cookie-events as they occurred.[2]

Participants also appeared to increase their awareness and understanding of cookies in a global context. In contrast to participants' self-assessment that their global understanding of cookies remained unchanged after the hands-on session, it was evident from participants 'talk-

[2] As noted in the retrospective analysis of browsers, users can obtain a comparable awareness of cookie-events as they occur if users enable a preference setting which queries the user about each individual cookie event. However, with this type of implementation the browser interrupts the user from the primary task with a modal dialog box each time a new cookie arrives and requires the user to explicitly accept or decline the cookie. Moreover, the dialog box does not present enough information about the incoming cookie to allow the user to make an informed decision. This interruption occurs for every cookie, even though sites typically set more than five cookies on a given page.

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

aloud' and unsolicited comments during the hands-on session that this was not always the case.

While the Cookie-Watcher appeared to contribute to the participants' global understanding, the Cookie-Information tool appeared less successful. Some participants failed to notice the Cookie-Information tool in its entirety. Of those who accessed the Cookie-Information tool, some did not read the text even though it was only four short paragraphs. Participants who did read the text found the language too technical for novice users, that the text did not adequately tie in with information presented elsewhere in the cookie tools, and that the text did not adequately convey a sense of benefits and risks from cookie use.

Participants also found the Cookie-Watcher, easy access to the Cookie-Management tools, and just-in-time information presentation to be a significant improvement over prior browsers for managing both individual and groups of cookies as they arrived. Observations of participant behavior and participant comments suggested that direct access to information on individual cookies from mouse events triggered in the Cookie-Watcher helped to reduce learning time as well as eased cookie management. Participants almost always examined and/or removed cookies as they arrived and were far less likely to return to a cookie from a previous site visit, even if that cookie was classified and displayed in a manner intended to attract the users' attention (third-party cookies for example). Participants also commented favorably on the option to ban sites from resetting cookies and one participant suggested an additional option to ban a site by manually entering its domain. In general, the cookie-management mechanisms present in this prototype were perceived to be far more efficient, effective, and intuitive than those found in other current browsers where one typically has to locate and hand-edit cookie files stored on the local machine.

In terms of traditional HCI measures for interface design, the cookie toolset interface was largely successful. Based on observation of participant behavior and participants' comments, participants were able to intuitively and readily use the new cookie tools with minimal effort and reasonable success. We also note some useful suggestions that arose from both the observations and interviews including: better separation of classification and cookie data; a re-examination of color and text choices in the representation of cookie events; use of icons and color gradients for redundancy of classification information; 'real estate' issues associated with the Cookie-Watcher; as noted above, the addition of an 'add domain' function for the Cookie-Watcher's 'banned' site panel; and a way to view the number of cookies set per domain.

As an overall measure of the success of the Mozilla Cookie-Watcher prototype in the post-session interview, seven of the participants (88%) stated that if such a toolset were available as an add-on to their browser of choice they would use it. One participant stated reservations about the use of the cookie toolset without a greater global understanding of cookies -- a comment with which the design team concurred.

7. Prototype three: the Mozilla Cookie-Watcher revisited

7.1. Description

Following the Value-Sensitive Design iterative methodology, we again revisited our design in light of our criteria for informed consent online, our design goals, and the results from the usability study. Based on these, we implemented several refinements to the Cookie-Watcher and Cookie Information Dialog Box (see Figure 3) as follows:

- The Cookie-Watcher no longer uses background color to represent both cookie domain and expiration information. Background color (green for same domain and red for third party cookie) is now used to represent cookie domain information. Font style (italics for within session duration; plain text for up to one year duration; and bold for more than one year duration) is now used to represent cookie duration.
- The Cookie-Information Dialog Box now contains a key to the color and font style representations of cookie information for domain and duration respectively.
- The Cookie-Information Dialog Box now contains information about the potential benefits and risks associated with a cookie by type of domain and duration. For example, a cookie from the Web site the user is currently visiting that will last only for the current session allows for personalization during this one visit but poses no risks for tracking within or across sites.

7.2. Formative Evaluation

We are currently conducting usability tests with Prototype Three. Preliminary results are positive. Shortly, we intend to install this version on several individuals' machines to be used as the primary browser. In addition to attending to traditional usability concerns, the evaluation will focus on Prototype Three's impact on the user's global understanding of cookies including common patterns for cookie deployment and potential

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

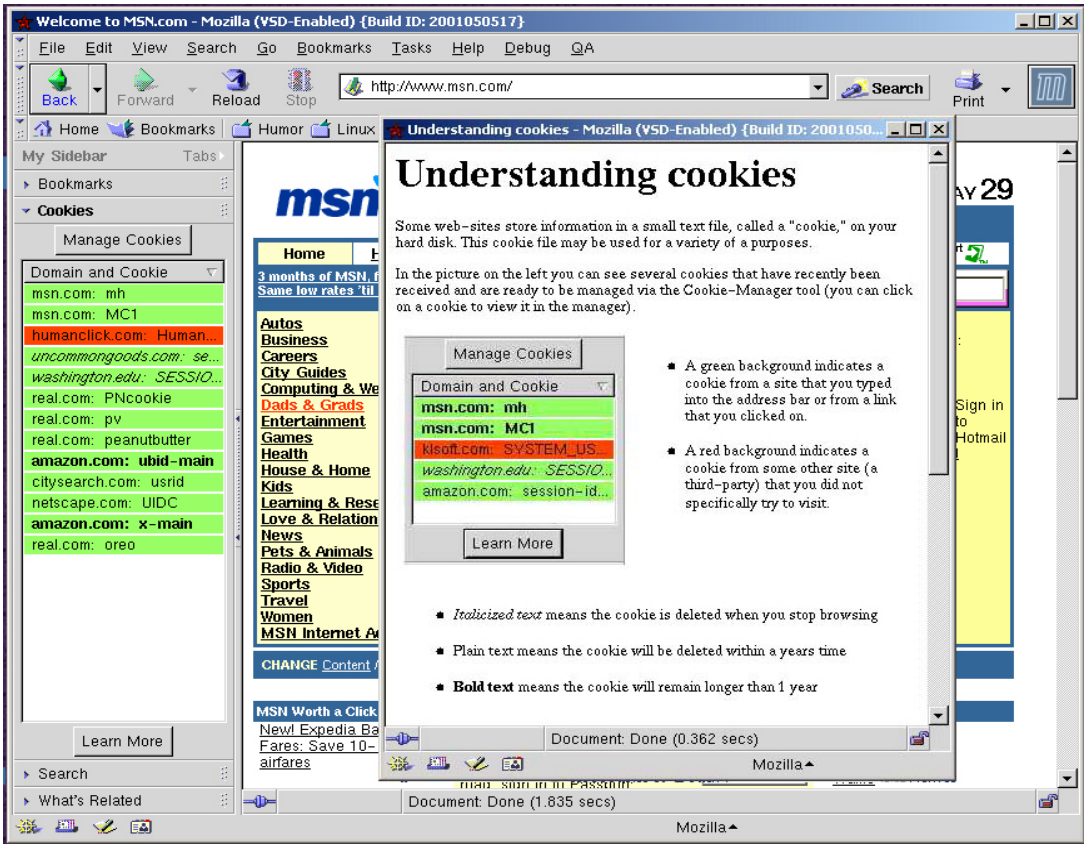

Figure 3. The Mozilla Cookie-Watcher prototype Revisited implemented in Mozilla showing the revised Cookie-Watcher tool (at the left) and the revised Cookie-Information Dialog Box (in the center).

benefits and risks associated with different types of cookies.

8. Conclusions

Informed consent is an important human value to integrate into our online interactions. However, doing so depends on the existence of underlying technical mechanisms to support the activities of "informing" and "obtaining consent". In this research, we have demonstrated with an implementation in the Mozilla browser how specific technical mechanisms – of peripheral awareness and just-in-time interventions – can be employed to support informed consent for cookies in the context of individuals' Web browsing. These mechanisms follow from our design goals to enhance users' local understanding of cookies, global understanding of cookies, and cookie management, all with minimal distraction from the task at hand. In turn, these design goals follow from our criteria for informed consent in online interactions as developed in prior work. Our formal evaluation efforts – particularly the usability study conducted with Prototype Two – suggest we have been largely successful in meeting these goals.

Our work is on-going. In the near term, we anticipate conducting longer-term evaluation studies of the currently modified Mozilla browser in labs, offices and participants' homes and with individuals who possess a wider range of experience, backgrounds, and technical skills. In later stages, we will solicit feedback from the open-source community. An additional goal of the project is the potential integration of the Cookie-Watcher and Cookie-Information Dialog Box into the official Mozilla browser release.

In addition to providing an improved solution for cookies, browsers and informed consent, our work also demonstrates the viability of the Value-Sensitive Design methodology in the context of a real-world large-scale software system: a methodology in which, as designers, we move from conceptual investigations of relevant values, to the development of new technical mechanisms to support those values, to empirical validation of our technical work in light of the conceptual investigations, and back again to the refinement of our technical mechanisms. It is our hope that in providing a large-scale real-world example of the Value-Sensitive Design methodology in action -- from theory through implementation and formative evaluation, and back again -- other researchers, designers, and engineers may more easily adopt aspects of Value-Sensitive Design methodologies and apply these to a wide range of problem domains.

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE

9. Acknowledgments

Austin Henderson, Lynne Henderson, David Hurley, and Valerie Wonder contributed to early discussions related to this work. This research was funded in part by National Science Foundation Awards IIS-9911185 and SES-0096131.

10. References

1. M. Ackerman, and L. Cranor, "Privacy critics: UI components to safeguard users' privacy", *CHI99 Extended Abstracts*, ACM Press, New York, 1999, pp. 258-259.
2. *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.
3. Bjerknes, G., Ehn, P., and Kyng, M., (Eds.), *Computers and Democracy: A Scandinavian Challenge*, Avebury, Aldershot, England, 1987.
4. Borgman, C. L., *From Gutenberg to the Global Information Infrastructure: Access to Information in the Networked World*, The MIT Press, Cambridge, MA, 2000.
5. L. Cranor, and P. Resnick, P., "Protocols for automated negotiations with buyer anonymity and seller reputations", *Netnomics,* 2000, *2(1)*, pp. 1-23.
6. P. Ehn, and M. Kyng, "Cardboard computers: Mocking-it-up or hands-on the future", in J. Greenbaum and M. Kyng (Eds.), *Design at Work: Cooperative Design of Computer Systems*, Lawrence Erlbaum Associates, Hillsdale, NJ, 1991, pp. 169-195.
7. Faden, R, and Beauchamp, T., *A History and Theory of Informed Consent*. Oxford University Press, New York, NY, 1986.
8. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (A Report to Congress). Federal Trade Commission, Washington, D. C., 2000, May.
9. Friedman, B., (Ed.), *Human values and the design of computer technology*. Cambridge University Press, New York, and CSLI, Stanford University, Stanford, 1997.
10. Friedman, B., *Value-Sensitive Design: A Research Agenda for Information Technology*, (Contract No: SBR-9729633), National Science Foundation, Arlington, VA, 1999.
11. B. Friedman, and P. H. Kahn, Jr., "A Value-Sensitive Design approach to augmented reality", in W. Mackay (Ed.), *Design of Augmented Reality Environments*, The MIT Press, Cambridge, MA, in press-a.
12. B. Friedman, and P. H. Kahn, Jr., "Human values, ethics, and design", in J. Jacko and A. Sears (Eds.), *Handbook in Human-Computer Interaction*, Lawrence Erlbaum Press, Mahwah, NJ, in press-b.
13. B. Friedman, P. H. Kahn, Jr., and D. C. Howe, "Trust online", *Communications of the ACM,* 2000, *43*(12), pp. 34-40.
14. Friedman, B., Millett, L., and Felten, Ed, *Informed consent online: A conceptual model and design principles*, UW-CSE Technical Report 00-12-2, 2000.
15. B. Friedman, and H. Nissenbaum, "Bias in computer systems", *ACM Transactions on Information Systems*, 1999, *14(3),* pp. 330-347.
16. L. Fuchs, "AREA: A cross-application notification service for groupware", *6th ECSCW Proceedings,* Kluwer Academic Pub., Dordrechet, Germany, 1999, pp. 61-81.
17. Greenbaum, J., and Kyng, M., (Eds.), *Design at Work: Cooperative Design of Computer Systems*, Lawrence Erlbaum Associates, Hillsdale, NJ, 1991.
18. Harris Poll/Business Week, "A growing threat", *2000.* http://www.businessweek.come/2000/00_12/b3673010.htm
19. S. E. Hudson, and I. Smith, "Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems", *CSCW '96 Proceedings,* ACM Press, New York, NY, 1996, pp. 248-257.
20. S. Iacono and R. Kling, "Changing office technologies and the transformation of clerical jobs", in R. Kraut (Ed.), *Technology and the Transformation of White Collar Work*, Lawrence Erlbaum, Hillsdale, NJ, 1987.
21. L. D. Introna, and H. Nissenbaum, "Shaping the Web: Why the politics of search engines matters" *The Information Society,* 2000, *16*, pp. 169-185.
22. E. A. Isaacs, J. C. Tang, and T. Morris, "Piazza: A desktop environment supporting impromptu and planned interactions", *CSCW '96 Proceedings*, ACM Press, New York, NY, 1996, pp. 315-324.
23. D. G. Johnson, and K. Miller, "Ethical issues for computer scientists and engineers", in A. B. Tucker, Jr. (Ed.-in-Chief), *The Computer Science and Engineering Handbook*, CRC Press, 1997, pp. 16-26.
24. Johnson, J., *GUI Bloopers: Don't and Do's for Software Developers and Web Designers*. Morgan Kaufman Publishers, 2000.
25. R. Kling, H. Rosenbaum, and C. Hert, "Social informatics in information science: An introduction", *Journal of the American Society for Information Science,* 1998, *49*(12), pp. 1047-1052.
26. Kyng, M., and Mathiassen, L., (Eds.), *Computers and Design in Context*, The MIT Press, Cambridge, MA, 1997.
27. L. Millett, B. Friedman, and E. Felten, "Cookies and Web browser design: Toward realizing informed consent online", *CHI 2001 Proceedings,* ACM Press, New York, 2001, pp. 46-52.
28. J. H. Moor, "What is computer ethics?" *Metaphilosophy,* 1985, *16*(4), pp. 266-275.
29. Nielsen, J., *Usability engineering*, Academic Press, Boston, MA, 1993.
30. J. S. Olson, and S. Teasley, "Groupware in the wild: Lessons learned from a year of virtual collaboration", *CSCW '96 Proceedings*, ACM Press, New York, NY, 1996, pp. 419-427.
31. W. J. Orlikowski, "Learning from *Notes*: Organizational issues in groupware implementation", *The Information Society,* 1993, *9*(3), pp. 237-250.
32. Rogerson, S., and Bynum, T. W., (Eds.), *Information Ethics: A Reader*, Blackwell Publishers, Cambridge, MA, 1999.
33. M. Weiser, and J. S. Brown, "Designing calm technology", *PowerGrid Journal,* 1996, *1*(1), http://powergrid.electriciti.com/1.01 .

Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)
0-7695-1435-9/02 $17.00 © 2002 IEEE