Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements

Nathaniel S. Good[1], Jens Grossklags[1],Deirdre K. Mulligan[2], Joseph A. Konstan[3]

[1]School of Information, UC Berkeley
102 South Hall, Berkeley, CA
{ngood,jensg}@ischool.berkeley.edu

[2]Boalt School of Law, UC Berkeley
346 Boalt Hall, Berkeley, CA
dmulligan@law.berkeley.edu

[3]Department of CS&E, University of Minnesota
200 Union Street SE, Minnesota, MN
konstan@cs.umn.edu

ABSTRACT

Spyware is an increasing problem. Interestingly, many programs carrying spyware honestly disclose the activities of the software, but users install the software anyway. We report on a study of software installation to assess the effectiveness of different notices for helping people make better decisions on which software to install. Our study of 222 users showed that providing a short summary notice, in addition to the End User License Agreement (EULA), before the installation reduced the number of software installations significantly. We also found that providing the short summary notice after installation led to a significant number of uninstalls. However, even with the short notices, many users installed the program and later expressed regret for doing so. These results, along with a detailed analysis of installation, regret, and survey data about user behaviors informs our recommendations to policymakers and designers for assessing the "adequacy" of consent in the context of software that exhibits behaviors associated with spyware.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces: *interaction styles, standardization, user-centered design*
J.4 [**Social and Behavioral Sciences**]: *psychology*
K.4.1 [**Computers and Society**]: Public Policy Issues – *privacy and regulation*
K.5.2 [**Legal Aspects of Computing**]: Governmental Issues – *regulation*

Author Keywords

Privacy, Security, Notice, End User License Agreement, Timing, Spyware

INTRODUCTION

Spyware, broadly defined, is fundamentally a challenge for HCI research as much as it is a technical one. At its core, fully disclosed spyware presents users with a trade-off: users gain the functionality of software in exchange for giving up private data, tolerating advertising messages, or both. While some examples of spyware are primarily fraudulent, others disclose the functionality of the spyware in a manner similar in form to the disclosure practices generally found in the software industry. Individual users have different needs and tolerances, and in the absence of public policy limiting their choices, the disclosures provided by spyware vendors would provide the basis for individuals to effectuate their policy choices in the marketplace. In an ideal market users would make decisions to install software, including spyware, where the trade was in their interest.[1] At times law constrains individual choice based on externalities or other market failures, or normative decisions about the values at issue. In the U.S., with respect to privacy and other issues commonly dealt with in mass-market software contracts there is little constraint on the substantive terms with respect to privacy, reliability, or security that can be presented to consumers.

It is not an ideal world. Study after study shows that people unwittingly install malicious or unwanted software [4][13]. It is easy to identify reasons for this disconnect. Certainly some of it is due to the software not disclosing what it does. Equally certainly, most users don't bother to read the lengthy and legalistic End User License Agreements (EULAs) or Privacy Agreements[27]. Even if the EULA is accurate, and the user reads it, the agreements may be so long and confusing as to prevent meaningful knowledge and consent. Some users may mistakenly believe that their operating system, antivirus software, or other precautions will protect them. But there are other reasons. Users may be too eager to use the software to be concerned about spyware—at least at that moment. And users who have just selected the action to install may be too committed to that

[1] We want to emphasize that we do not wish to downplay the problems associated with malicious software that fails to disclose its true behavior; as we discuss below, there are legal remedies for such deception. However, in this work we restrict our attention on supporting users in making correct decisions when faced with disclosed trade-offs.

action to suddenly change course (just as Norman suggests that immediate confirmation of deleting a file is useless or worse [22]).

Our work builds upon a previous study of 31 subjects that showed that short summary notices, as a supplement to EULAs, have promise in helping users identify which software they feel comfortable installing [18]. We studied 222 subjects, observing their installation behavior in one of three information conditions: 1) an ordinary EULA, 2) a short summary notice before installation additional to the EULA, 3) a short summary notice (with an opportunity to uninstall) immediately after installation additional to customary EULA. We also surveyed users about their behavior in both computer use, more general use of legal documents (e.g., signing such documents without reading them) and actions regarding several online risks. The results of this study provide significant opportunities for designing software systems that better support users in protecting themselves against unwanted spyware, and might even generalize to a broader set of "in-the-moment" decisions.

The fact that users do not read EULAs may appear to be a truth in need of little proof. But for the current policy debates this finding is important. The courts, absent fraud or unconscionability, largely hold individuals responsible for the terms of legal agreements regardless of this reality. However, because a defining element of spyware is the context—in particular the consent experience—around its acquisition state and federal regulatory agencies and the private sector are developing new policy that establishes procedures aimed at providing an "adequate" consent experience. While reflective of HCI in some respects there has been little transfer of knowledge or prior research to determine the likely effect of these enhanced procedural rules. Thus, there is much to be gained from a cross-disciplinary conversation around the HCI contributions toward these reforms.

RELATED WORK

As some experimental research demonstrates, users stated privacy preferences do not always align with their behavior [2][23]. For small monetary gains (e.g., a free program) or product recommendations, users are willing to trade off their privacy and/or security [2][23]. Moreover, users are more likely to discount future privacy/security losses if presented with an immediate discount on a product [2]. Notices often fail to dissuade individuals from making decisions that contradict their own clearly stated preferences [23][27].

HCI practitioners have been concerned about privacy concerns on the web in general, and recent work in HCISec (HCI and security)[2] has been concerned with cookie management [15][16], spyware [24], phishing [12], as well as online privacy notices [10][20] and incidental privacy issues with web browsing [19] and filesharing [17].

HCI practitioners are uniquely positioned to contribute to the conversation on designing more effective notices by, for example, improving on timing and visualization. However, contributions to notice design are challenging because users are simply trained to ignore consent documents. This challenge of attracting attention to important events is not a new one in HCI. A number of researchers are studying the effects of notification systems in computing. They examine the nature of interruptions and people's cognitive responses to work-disruptive influences. Notification systems commonly use visualization techniques to increase information availability while limiting loss of users' focus on primary tasks [11][26][25]. From control room and cockpit indicators to desktop notifiers, substantial research has been devoted to identifying visual and auditory displays that attract attention and to designing interaction sequences that prevent automatic dismissal of information.

Work on privacy notices for web sites spans several different areas. P3P[3] and privacy bird[4] were popular efforts to inform users about a Web site's privacy preferences, as well as to give users control over the types of information exchanged with interaction partners. The P3P design called for web designers and companies to provide easy to read, privacy statements in a standard format that is usable, for example, by P3P-aware browsers to communicate this information to the end user.

Recent research by Karat *et al.* [21] aims at providing design methodologies and tools to assist in the creation of more usable privacy policies that can be verified by automated techniques. A main objective is to achieve consistency between notices, as well as better compliance with emerging privacy standards.

Friedman *et al.* [15] work towards improving interfaces for informed consent through implementing value sensitive design methodologies. Their design approach targets users' comprehension and suggests methods to facilitate consent between the user and the application based on shared knowledge and trust.

Early work with privacy in HCI was focused on the notion of feedback and control, introduced by Bellotti and Sellen [6]. The concept of feedback and control suggests that users are given ample feedback on the actions a system is taking, whether it is video taping someone or sending information to a third party, and that users are given adequate means of

[2] See the HCISec Bibliography for the most important contributions to this field. http://www.gaudior.net/alma/biblio.html

[3] W3C Platform for Privacy Preferences Initiative. Platform for Privacy Preferences (P3P) Project. http://www.w3.org/P3P.

[4] http://www.privacybird.com/

controlling the flow of this information, such as being able to turn off recording or specify which information is sent to third parties.

The concept of feedback and control is related to the legal explanations of informed consent. Informed consent emphasizes that end users must receive notice (signs, readable language, etc.), and must be able to provide consent to the action. Essentially, to use a term in contracts, both parties have to establish a "meeting of the minds" where they are both consenting to and are agreeing to the same shared set of knowledge.

Courts typically enforce EULAs. Courts have enforced shrinkwrap agreements that purport to bind users to EULA terms that appear on software packaging simply because the user opened the package.[5] Courts typically find that installing or using the software is sufficient to establish acceptance of EULA terms even when users are not required to click "I Agree."[6]

There is a growing body of literature questioning the courts generally unquestioning and superficial review of the context of contract formation, specifically around notice and consent. Within the legal literature and policy circles questions about the adequacy of consent, in particular the form, content, presentation and timing of disclosures in relation to programs that exhibit behaviors associated with spyware, are being raised [14][7][8][28][29][5][3][1].The Federal Trade Commission and the State Attorney Generals are challenging the courts' laissez-faire attitude towards contract formation demanding heightened procedural, and to a lesser extent substantive, protections for contract formation in the context of spyware enforcement actions. The rules they are establishing in this context will likely inform the agencies, and in time the courts, views on contract formation with respect to downloadable software in general.

Given the connection between the privacy and security decisions of individual users and the overall security of the network, the questions about externalities bear particular attention. If we are to rely on a private contractual approach to privacy in the U.S. we need to make sure that private choices don't undermine collective security and that users are capable of understanding and making the privacy and security decisions necessary to protect their interests.

Our report adds to the growing literature on HCI and security/privacy but also makes important connections to the ongoing legal and policy reforms around notice and consent.

[5] *Bowers v. Baystate Technologies, Inc.* , 320 F.3d 1317 (Fed. Cir. 2003).

[6] See Tarra Zynda, Note, *Ticketmaster Corp. v. Tickets.com, Inc.: Preserving Minimum Requirements of Contract on the Internet*, 19 Berkeley Tech. L.J. 495, 504-505 (2004).

EXPERIMENTAL DESIGN

Experimental Setup

Our experimental setup consisted of an experimental portion, followed by two surveys. Subjects were given a unique number, and sheet outlining the basic scenario of the experiment. All of the experiments and surveys were done by each subject independently on a computer located in a laboratory with dividers. As the user passed each portion of the experiment, the application would record the actions and provide the next portion of the experiment. We describe the details of each portion of the experiment below.

Experimental Framework

The experimental portion of our framework was designed to mimic the experience of installing software applications, but also allows us to modify the notice and consent process encountered. Previous experiments showed us that pop-up windows and warnings are quickly ignored by users who are accustomed to click through them. In order to have users "notice" the notice conditions, we decided to build them into the install experience.

We constructed a windows application in C# that would not only depict the installation process as realistic as possible, but also log all user actions (e.g., buttons clicked, time per screen) during the study. Additionally, the application we constructed would provide a launching pad that could dynamically configure each subject's experience based on their user number we provided at the beginning of the experiment. Users were given a user id, which was matched up against a list of acceptable identifiers and associated with a treatment and a counter-balanced program ordering.

We constructed two surveys, which could be accessed from the application launching pad. After the experimental portion was completed, users could click on the survey buttons to answer each respective survey. When both surveys were completed, the user was returned to the launching pad, and told that the experiment was completed.

Notice Treatments

Our design consisted of three notice conditions: two treatments with customized short notices that included abbreviated EULAs for the programs plus the original EULA (all without brand information) and one control condition that only consisted out of the original EULA (again all without brand information):

PRE - Short notice before installation presented on the Install Option Screen plus the original EULA on the EULA screen;

POST - Short notice after installation on the Post Install Warning Screen plus the original EULA on EULA screen; and

CONTROL/None - No short notice at all, but with the original EULA on the EULA screen.

Each notice condition was integrated into three programs with consistency maintained for each portion of the controlled experiment by providing similar screens, but changing the content of the information in key screens for the different programs. Figure 1 below details the screens involved in the installation process for each user.

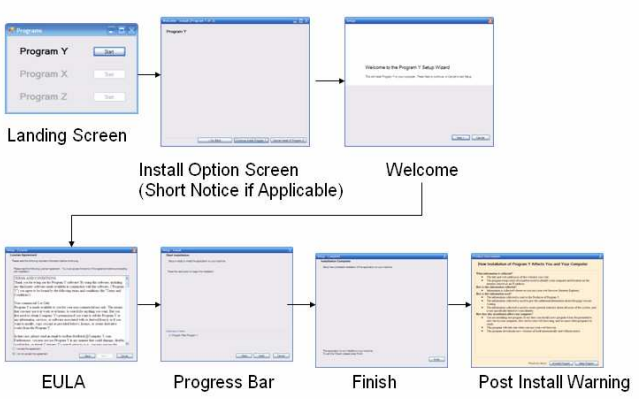


Figure 1 Process of installation screens in experiment

The Post Install Warning screen only occurs when a user is in the post notice condition. However, the Install Option Screen displays the Short Notice in the Pre condition, but appears also in the other two treatment conditions without specific information. At any time, a user may cancel the installation and return to the landing screen to start with the next program. Additionally, users may move back and forth between screens as in typical installation programs by hitting the back key.

We selected programs from our previous study [18] to facilitate comparability of the results and user experience. We chose a browser toolbar, a weather information service and a file sharing application. For the experiment each brand name was removed and replaced with a generic title. The program titles and descriptions are listed below:

- Program X – Weather Information Program
- Program Y – Browser Toolbar
- Program Z – File Sharing Program

To summarize, we ran a 3x3 mixed methods study, consisting of 3 *between*-subjects factors and 3 *within*-subjects factors. The between subjects factor were the notice conditions (None/Control, Pre, Post) and the within-subjects factors were the programs (Filesharing, Weather Service and Browser Toolbar). Within subjects factors were counter-balanced within the population. We want to add that it is of methodological interest to us to understand the relative strengths and weaknesses between the small scale user study and the current large experiment with hundreds of users.

Notice Construction

Our short notices were designed by distilling the long EULAs from three programs included in our study. We used the same short notices as we constructed in a previous study. Each notice condition that included a short notice (Pre and Post) had the same text for a specific program. The only difference between each treatment was the timing where each notice was shown. Examples of how the short notice for Program Z would appear during the experiment in the pre-notice and post-notice treatments are presented in Figure 2 and Figure 3, respectively.

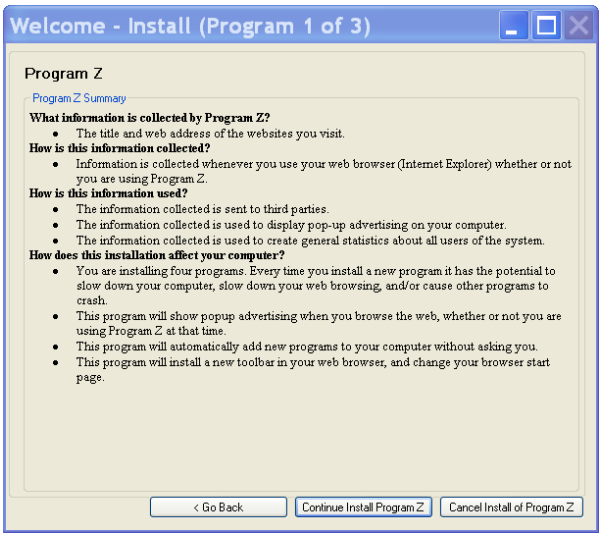


Figure 2 Pre-installation short-notice (would appear on Install Option Screen in Pre-Notice treatment)

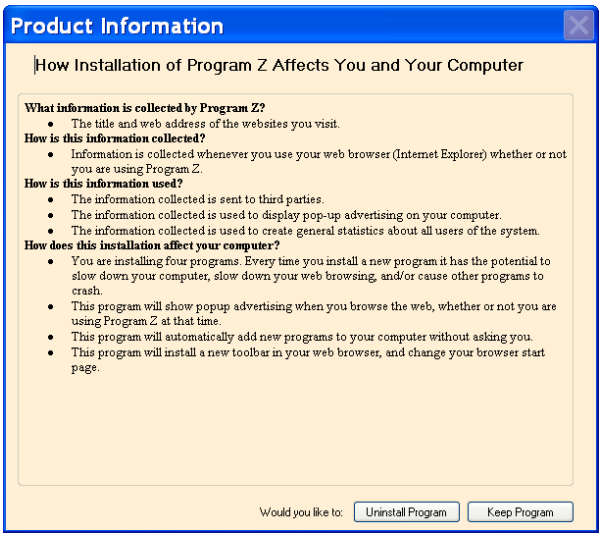


Figure 3 Post-installation short-notice (would appear on Post Install Warning Screen in Post-Notice treatment)

Surveys

Our study included two surveys that were presented to the user after the installation experiment. The surveys included different question types, for example, open ended, Likert

scales, and simple yes/no questions. The purpose of the survey was to understand the subjects' concerns regarding a representative selection of online risks and stated behaviors related to software notices, as well as to determine how the users perceived the programs in the experiment as well as whether or not they regretted the actions they performed in the experiment after being provided with an (additional) chance to review the short notice.[7]

The first survey consisted of demographic and behavioral information, while the second survey consisted of questions regarding the experimental experience. In total, we anticipated that the two surveys plus the experiment section could be passed by the average subject in about one hour.

Table I Self-reported behavior regarding online risks

	Total	
	Mean	Std. Deviation
Try Functionality	4.41	2.64
Research on Web	5.14	2.64
Once Installed wont remove	2.24	1.72
Accept Popups for free stuff	3.36	2.42
Install programs that look interesting	3.55	2.35
Install only if I know exactly what it does	6.41	2.06

RESULTS

Subjects

240 subjects participated in the study, of which we were forced to remove some entries due to missing data leaving us with 222. Subjects were paid $20 for their participation, and were recruited by a university service with access to a subject pool of several thousand students. Our subjects are divided into three treatment groups: 64 users in the control condition, 80 in the pre-notice condition and 78 in the post-notice condition. We used chi-squared to analyze differences between the discrete variables of install and regret, and ANOVA to analyze the differences between the continuous variable of time.

64.2% percent of our subjects were female. 39.5% indicated their age as less than 20 years-old. An additional 57.7% were between the ages of 20 and 25. The dataset also includes a small group of 2.7% over 25 years of age. On average we had a very computer-experienced group of users. For example, 85.2% stated that they maintained their home computer themselves.

[7] Of course, subjects in the control group and those in the post notice treatment that canceled early had not seen the notice before.

Attitudes towards online risks

We asked users to rate concerns on a scale of 1-9, with higher numbers expressing more concern. Subjects expressed high concern towards 5 different risk types and nuisances often encountered in online interactions: identity theft, spyware, viruses, pop-up advertisements, and privacy intrusions.

Surprisingly, our young subject pool was somewhat less alarmed about identity theft and privacy compromises, compared to being subject to spyware attacks and pop-up advertisements. Possible damages caused by viruses topped the list.

We employed *k*-means multivariate clustering techniques to classify subjects according to their risk attitudes. Hierarchical clustering (single linkage) preceded the data analysis. We selected the best partitioning using the Calinski-Harabasz criterion [9]. We derived two distinct clusters: a first group with a substantially higher degree of unease about online risks along all measured dimensions (62.2%) and a second less worried and comparatively smaller group (37.8%).

Self-reported behavior regarding online risks

Our subjects are forthcoming about their good computer hygiene practices (see Table I; values are reported on scale from 1-9). On average, while they are interested in trying new content, they report to somewhat often research programs on the Web before using them, claim that they only install program when they are well informed about them, and report that they hardly leave them installed if found undesirable. They rarely agree with the statement that free software in exchange for intrusive advertisements is acceptable. Only few wholeheartedly admit that they would frequently download and install programs that look interesting.

Self-reported reading practices for legal documents

Only very few users reported reading EULAs often and thoroughly when they encounter them (1.4%). Members of a larger group categorize themselves as those who often read parts of the agreement or browse contents (24.8%). However, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them.

Table II Self-reported reading practices for legal documents

	Total	
	Mean	Std. Deviation
Financial Privacy Notices	5.97	2.78
Read Web Privacy Notices	4.24	2.28
Read Shrinkwrap Licenses	3.81	2.25

In Table II we report on subjects' reading behavior for other important notices (values are reported on a scale from 1-9 from "never read" to "always read". Web privacy notices and shrinkwrap licenses are read less frequently in comparison to, for example, financial privacy notices. Less related to our field of investigation, we found that food nutrition labels and credit card statements are read almost twice as often as shrinkwrap licenses by our subject group (means of 6.8 and 7.3, respectively).

Table III Occurrences of canceled installations for each screen

Treatment	Cancellation Screen	Program X	Program Y	Program Z
None	Install option	15.6%	9.4%	9.4%
	Welcome	15.8%	0.0%	0.0%
	EULA	4.7%	0.0%	4.7%
	Install Progress	0.0%	0.0%	0.0%
	TOTAL CANCELED	32.1%	9.4%	9.4%
Pre	Install option	69.2%	28.2%	69.2%
	Welcome	1.2%	0.0%	0.0%
	EULA	0.0%	0.0%	0.0%
	Install Progress	0.0%	0.0%	0.0%
	TOTAL CANCELED	70.4%	28.2%	69.2%
Post	Install option	13.8%	2.5%	11.3%
	Welcome	0.0%	0.0%	1.3%
	EULA	11.3%	1.3%	5.0%
	Install Progress	1.3%	0.0%	0.0%
	Post Install Warning	51.3%	28.6%	58.8%
	TOTAL CANCELED	77.7	32.4%	76.4%

Behavior in the experiment: Installation

Chi-squared tests showed that both notice conditions had significantly lower instances of installation than the control condition ($p<.001$). This effect is robust independent of whether the unit of investigation are the whole treatment groups or individual programs ($p<.001$)

This result demonstrates that the short notice treatments had a significant behavioral impact on subjects. It also supports what we have seen in previous studies and have observed in the field - users that are presented with the omnipresent overly long and complex presentation of EULAs are prone to installing applications more often. As we saw in our previous small-scale ecological user study[18], the toolbar application was most frequently installed, followed by the file sharing application and finally the weather information service. For the control treatment we attribute the difference between programs to a combination of two effects: preference for a program type (e.g., toolbar vs. filesharing client) vs. desirability of contractual terms. Users seem to be able to discriminate between programs even without additional cues such as brand information and familiar user interface design. The results we present in following sections rest on the variation of treatment variables.

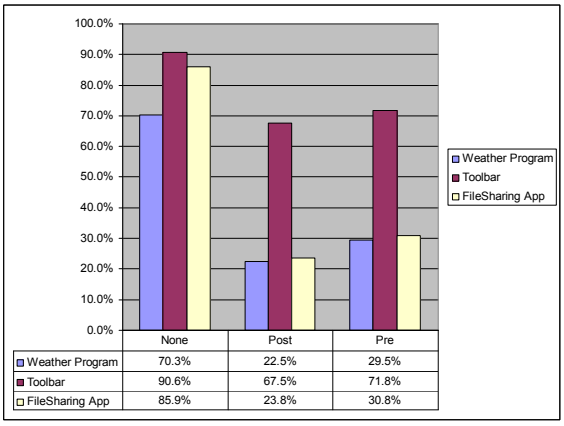


Figure 4 Programs installed by users

Behavior in the experiment: Cancellations/Uninstalls

Interestingly, of those that canceled the installation in the control and post-notice treatments the preferred action (always more than 50%) was to leave the program immediately on the very first screen (that is Install option screen). Only between 0% and 42.8% of subjects ended up visiting the EULA screen. This result is of importance for program developers interested in increasing their installed base. It seems that although many people might enter an installation they often will immediately leave even without gathering further information.

Table III reports the percentage of all individuals that canceled on particular screens for the three different treatments. It demonstrates the dominance of the short notice screens (Install Option for pre-notice and Post Install Warning for post-notice) in comparison to the EULA screen.

Note that the short notices contained information from the original EULA, however, presented in a unified and abbreviated format. Therefore, the data for the post notice treatment clearly demonstrates the inadequacy of the long and complex EULA. All subjects that canceled on the Post Install Warning screen have seen the original EULA on the screens they passed to reach the warning screen. But only on the short notice screen they decided to cancel.

Behavior in the experiment: Timing and reading notices

Pre-notice

In our experiment there is only one screen per program that was visited by everybody independent of treatment condition and whether they installed or canceled the installation at some point of the process. This is Install Option Screen. In Table III we have already shown that

many subjects decided to cancel at this point of installation. It, however, is also interesting to note that there are significant differences in time spent by the subjects at this point of the experiment.

Table IV Time in sec for Install Option Screen (Program X)

Treatment	Installation completed	Mean time (sec)
None	Yes	1.9
	No	13.5
	Significance result	p<0.0037
Pre	Yes	3.4
	No	59.2
	Significance result	p<0.0000
Post	Yes	0.5
	No	8.3
	Significance result	p<0.0002

First, individuals that decided not to install a program are significantly slower than installers for all three treatments (see Table IV).[8]

Second, not surprisingly, individuals that do not install the programs spent more time on the Install Option Screen if they are members of the pre-notice treatment group compared to those in the control or post-notice treatments (with at least $p<0.05$ for all programs, but stronger for most). They are obviously paying attention to the notice.

Third, for those that installed the programs there is no such statistically significant difference noticeable. It should be added that installers in the pre-notice condition also passed quicker through the Install EULA screen than the control and post-notice group; that is, they did not pass quickly through the pre-notice screen with the intention of reading the actual EULA carefully.[9] Accordingly, they are consistently quicker than others. Or, to phrase it differently, they are ignorant towards notices.

We conclude that one main difference between installers and those that decline the program offerings is the time they spent deliberating at the start of the program installation. Even for the two treatments where no pre-notice was displayed on the Install Option Screen non-installers are considerably slower. One interpretation is that more deliberate individuals take additional time to study the short notice.

[8] Result does not hold for program y in the control treatment. However, the group of non-installers is extremely small for this program which makes it an outlier case.

[9] The group mean comparison test is significant for program x and z ($p<0.005$). For program y the differences have the expected direction, however, are not significant.

Table V Comparison of pre and post-notice reading time

Program installed	Cancellation Screen	Time for Program X (in sec)	Time for Program Y (in sec)	Time for Program Z (in sec)
Yes	Mean Pre-notice	3.4	8.5	0.0
	Mean Post-notice	14.5	35.6	15.6
	Significance	p=0.01	p<0.0000	p<0.0000
No	Mean Pre-notice	59.2	81.0	44.2
	Mean Post-notice	30.2	37.1	30.8
	Significance	P<0.0000	p<0.0006	p<0.005

Post-notice

Finding a natural comparison standard for the reading time in the post-notice treatment is more difficult since the Post Install Warning Screen appeared only in this treatment. We believe that comparing pre-notice and post-notice reading time is the most natural approach.

Table V strongly supports the finding that individuals who eventually installed a program passed slower through the Post Install Warning screen compared with the Install Option Screen. However, subjects that did not install a particular program took more time reading the pre-notice.

Assuming that increased reading times improve consumer decision-making this demonstrates a conundrum. On the one hand, we observed for the pre-notice that only non-installers read the notice (or even become aware of the notice). This is different for the post-notice where reading times even for subjects that completed installations are significantly distinct from zero. On the other hand, if subjects became aware of the pre-notice they spent a considerably longer amount of time absorbing the information which usually led to a cancellation of the installation process.

From a behavioral point of view it appears that subjects are very much willing to cancel an installation at the beginning of the process if they are adequately informed about the terms of the transaction. However, the risk is that they are too involved in the flow of conducting the necessary installation steps in order to notice the additional warning terms.

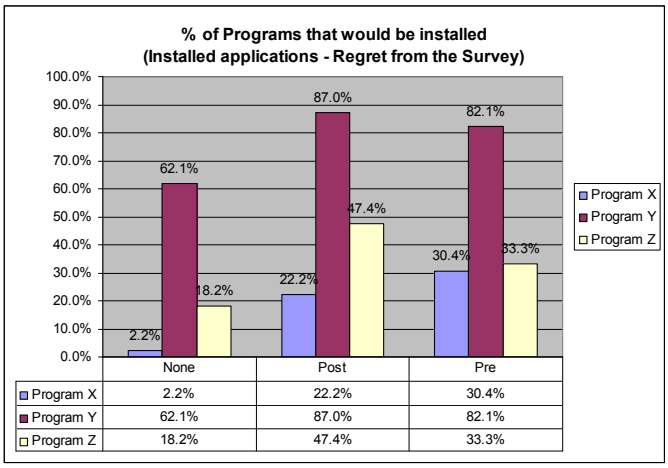
In contrast, the post-notice serves to slow down a majority of the individuals. It seems that subjects at this time of the installation process are able to notice and digest further information; that is, they have left the flow state. However, reading the notice does not necessarily result in the uninstallation of the program. One interpretation is that subjects have made an emotional investment into the program installed. Or they might be interested in trying the program even if they dislike its terms since it is already

installed at this point. As a result, not all users are willing to reverse their decisions. Another potential explanation is that subjects who keep the program feel that it adequately reflects their preferences for a consumer program. The distinction between these hypotheses is left for future work, but we present further evidence on this question in the next section.

Correlation Survey and Experiment: Regret

In Post Survey 2, we showed all subjects the short notice for each program, and asked them if they would install the program described in the short notice or not. We used this measure as a means of calculating the user's regret. In the post case, we calculated regret after users had seen the post notice, and had made the decision to keep or uninstall the program. We determined that users would have two types of regret, regret that they installed a program (and would like to remove it) and regret that they chose not to install a program (and they would like to install it). The second case we expected to be less common.

Overall regret was high for programs that users installed. Only in the case of program Y, the toolbar, do we see that over 50% of the users were happy with their installation choices. Regret is still very high for the programs that users consider the least usable, namely program X. In the best case, the pre notice, 70% of the users still regret installing the application. Although short notices may help, there is still much room for improvement.



	None	Post	Pre
Program X	2.2%	22.2%	30.4%
Program Y	62.1%	87.0%	82.1%
Program Z	18.2%	47.4%	33.3%

Figure 5 Graph of percent of users who were happy with their installation choices

Reading and Regret

The high regret we saw lead us to wonder as to whether regret was different in cases where users actually spent more time on the notice screens, either the short notices and/or the EULAs themselves. We decided to analyze cases where users had made it to at least one notice screen (EULA and/or short notice), and compared the time that users spent on each screen to their stated regret. By using time as an implicit measure of reading we were able to determine if the notice reading time had an effect on regret.

Overall, we found a strong difference between the control treatment and the pre treatment in terms of regret ($p<.05$). We found that in most cases, users who spend more time reading the short notices in both the pre and post conditions had less regret. Details of regret in each treatment condition are given below.

Regret and the Short Notice Condition

Not surprisingly, in the short notice case, we saw a significantly lower level of regret ($p<.05$) for users who spent more time reading. Users who had less regret spent on average 20 – 30 seconds more per notice, approximately double the average time in most cases.

Regret and the Post Notice Condition

At a first glance, the post notice condition seemed similar to the control condition. Because the post condition comes after users look at the EULAs, the combined post notice and EULA time may be dominated by behaviors we see in the EULA only case. For this reason, we ran another case where we separated the EULA time from the post notice time, and looked at how time on the post notice related to regret.

In this case, we found that the post noticed behaved similarly to the short notice, but the effect was not as strong across all program types. Users who spent more time on the post notice had significantly lower regret for the least desirable program, program X, but not across the other program types. We found this to be interesting because users in the post notice condition had to decide to keep the program or uninstall it. It was also the last notice that the users saw, so we were surprised that post notice had still had high cases of regret. It may be the case that for some users, after they have committed to an installation they feel they have some investment in the program or momentum and would like to continue to install. In the future, we plan to use more sophisticated modeling techniques to derive more comprehensive and powerful explanations of these kinds of user behavior.

Regret and the Control Condition

We found that in the control condition, users had a high amount of regret, whether they spent time reading the EULA or not across most programs. The control case, users had significantly higher values of regret ($p<.001$) for programs x and z. and a moderately higher value than the pre condition in program y ($p<.10$). In some cases, users who read more had significantly higher cases of regret than those that read less ($p<.05$). There is evidence that the EULAs could be confusing and misleading [18]. One user from our survey said she was "befuddled by the language" another mentioned that "they're often very very long [and] not easy reading, either." Users also mentioned that if they

have concerns, they look for certain terms such as “pop ups” or other things that may adversely affect their computer. One user mentioned “[I would look at them] if [they were] precise and clear, and the agreement is short, so it’s not too time-consuming. And the words are keywords, so I could just browse it very quickly at a glance. Besides, I will read it when the program alerts me the bad consequences of not reading the agreements.” This result emphasizes the need to have common terms across software licenses, especially for cases that deal with issues users are generally concerned about (performance, pop-ups, monitoring, etc).

Summary of Reading & Regret Results

From our analysis of reading and regret, we have learned that if we can get users to spend time reading the notices, they may experience significantly less regret. In this case, it is important for HCI practitioners to determine what can be done in terms of interfaces to get more users to slow down and read notices.

DISCUSSION

Observations and Implications

Four observations have very clear design implications for software installation systems and for efforts in the public and private sector to make the consent experience meaningful.

First, the experiment validates the use of short summary notices as a mechanism for reducing the installation of unwanted software. There are many ways in which such notices could be provided, ranging from legal solutions (where the use of such notices could be necessary for documenting informed consent) to technical and business ones (e.g., the creation of subscription services that provide such "installation reviews" for users). Efforts at state and federal regulatory agencies to simplify and highlight core software behaviors and draw attention to particular terms appear promising based on our research.

Second, the effectiveness of post-install notices suggests an alternative strategy for reducing unwanted spyware – delaying the actual irrevocable installation of software. Users might be well-served by systems that "pretend" to install software, then warn about the consequences before really completing the installation. (This approach could be a variant of the "to finish installation, you must reboot" barrier.) Or in some cases, it may even be worth preventing immediate use of software to provide a period of reflection. Efforts in the private sector to create virtual machines or sand boxes of sort that would allow consumers to test out software without allowing it fully onto their machine appear promising.

Third, from the regret data in the pre- and post-experimental conditions, we know that substantial regret exists even with these short notices. Accordingly, it is important to continue to explore other remedies to the spyware problem, including legal protections, technical protections, and interfaces that intercept the problem before the installation decision is made. Indeed, Google's warning that forces confirmation from people following a link to certain web sites (primarily cracking-related) could be adapted, or better yet, tools tied to ratings services could label links to software with indicators of the negative consequences of its use. It also points to the need for users to be provided with simple means to restore their machines to pre-installation state. Recent spyware enforcement actions have focused on this requirement.

In general, our research conclusions support the additional procedural constraints the FTC and State AGs are placing on spyware vendors. Given the contextual and individually subjective decisions about what is spyware our research would support the expansion of these protections to a broader range of software installations. The question is how broad a range is appropriate given that enhanced notices about everything is likely to undermine the utility and effectiveness of these “express consent” procedures where users face the greatest risks.

Finally, the presence of individual differences in reading behavior and other behaviors correlated with spyware installation suggests that personalized solutions have promise. Some users are well-served by the current system, or would be with short summary notices. Others seem likely to ignore such notices and might be willing to accept more restrictions on their installation (e.g., longer delays sequences of confirmations, or approval from another individual) in order to reduce their own risk and later regret. There are many paths to explore in this direction. To the extent that the overall security of the network is influenced by the decisions of users some of who ignore the processes established to engage them in good decision making, it is worth asking whether some private choices to tolerate spyware—particularly spyware that creates opportunities for others to remotely assume control of computers—are just too damaging to the network to remain in the realm of private choice.

FUTURE WORK

The research reported here opens as many questions as it resolves. It is our goal in future work to better understand the factors that lead individuals to install spyware, and how those factors vary in different demographic groups (including older users) and in different situations. We recognize the limitations of a laboratory study, and are hopeful that it will be possible to conduct more extensive studies of software installation, and more general questions of a personal computer's life cycle, on computers installed in individual homes and offices. Further, we believe that appropriate notice can help reduce installation of unwanted spyware, but also recognize that "appropriate" may vary by individual. We would particularly welcome further research into possible negative effects of excessively long

and impenetrable EULAs, and other explorations into interfaces for more effectively presenting the relevant information to users for meaningful, informed, consent.

ACKNOWLEDGEMENTS

We wish to thank Microsoft for funding our work. We also appreciate the help of Tye Rattenbury, Frances Tong and Xin Wang concerning statistical analysis. We are greatly indebted to Susheel Daswani for constructing the experimental framework. Finally, we thank Becca Shortle, Chris J. Hoofnagle, Ira Rubenstein and the anonymous reviewers for their valuable feedback and suggestions. This work is supported in part by the National Science Foundation under ITR award ANI-0331659.

REFERENCES

1. Abrams, M., M. P. Eisenhauer, and L.J. Sotto Letter to Federal Trade Commission. March 29, 2004. Re: alternative forms of privacy notices, project no. P034815. Hunton & Williams: The Center for Information Policy Leadership.
2. Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1): 26–33.
3. Anti Spyware Coalition, Anti Spyware Coalition Definitions and Supporting Documents, Working Report (June 29, 2006), available at http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf
4. AOL and National Cyber Security Alliance. 2004. AOL/NCSA online safety study, (October). http://www.security.iia.net.au/downloads/safety_study_v04.pdf
5. Bellia, P. L. Spyware and the Limits of Surveillance Law, 20 Berkeley Tech. L.J. 1283 (2005)
6. Bellotti, V. and A. Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In Proceedings of The Third European Conference on Computer Supported Cooperative Work (ECSCW'93). Milan, Italy: Kluwer Academic Publishers.
7. Blanke, J. M. "Robust Notice" and "informed Consent:" the Keys to Successful Spyware Legilsation, 7 Coum. Sci & Tech. L. Rev. 2 (2006)
8. Buenaventura, M. A. Teaching a Man to Fish: Why National Legislation Anchored in Notice and Consent Provisions is the Most Effective Solution to the Spyware Problem, 13 Rich. J.L. & Tech. 1 (2006)
9. Calinski, R.B. and Harabasz, J. 1974. "A Dendrite Method for Cluster Analysis," Comm. in Statistics, vol. 3, pp. 1–27.
10. Cranor, L.F., J. Reagle, and M. S. Ackerman.1999. Beyond concern: Understanding net users' attitudes about online privacy. In Ingo Vogelsang and Benjamin M. Compaine, eds. The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy. Cambridge, Massachusetts: The MIT Press, p. 47-70
11. Cutrell, E., M. Czerwinski, and E. Horvitz. 2001. Notification, disruption, and memory: Effects of messaging interruptions on memory and performance. Proceedings of Interact 2001: IFIP Conference on Human-Computer Interaction, Tokyo, Japan. http://research.microsoft.com/~cutrell/interact2001messaging.pdf.
12. Dhamija, R., Tygar, J. D., and Hearst, M. 2006. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). ACM Press, New York, NY, 581-590.
13. Earthlink. 2005. Earthlink spy audit: Results complied from Webroot's and Earthlink's Spy Audit programs, http://www.earthlink.net/spyaudit/press.
14. Federal Trade Commission, Monitoring Software on Your PC: Spyware, Adware, and Other Software, http:www.ftc.gov/os/2005/03/050307spywarerpt.pdf
15. Friedman, B., Howe, D., and Felten, E. 2002. Informed Consent in the Mozilla Browser: Implementing Value Sensitive Design. In Proceedings of the 35th Annual Hawaii international Conference on System Sciences (Hicss'02)-Volume 8 - Volume 8 (January 07 - 10, 2002). HICSS. IEEE Computer Society, Washington, DC, 247.
16. Goecks, J. and Mynatt., E.D. 2005. Supporting Privacy Management via Community Experience and Expertise, Proceedings of 2005 Conference on Communities and Technology, p. 397-418.
17. Good, N. S. and Krekelberg, A. 2003. Usability and privacy: a study of KaZaA P2P file-sharing. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM Press, New York, NY, 137-144.
18. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J. 2005. Stopping spyware at the gate: a user study of privacy, notice and spyware. In Proceedings of the 2005 Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 06 - 08, 2005). SOUPS '05, vol. 93. ACM Press, New York, NY, 43-52
19. Hawkey, K. and Inkpen, K. M. 2006. Keeping up appearances: understanding the dimensions of incidental information privacy. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). ACM Press, New York, NY.
20. Jensen, C., and C. Potts. 2004. Privacy policies as decision-making tools: An evaluation on online privacy notices. In CHI 2004 Connect: Conference Proceedings: April 24-29, Vienna Austria: Conference on Human Factors in Computing Systems 6(1): 471–78. New York: Association for Computing Machinery.
21. Karat, C., Karat, J., Brodie, C., and Feng, J. 2006. Evaluating interfaces for privacy policy rule authoring. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson, Eds. CHI '06. ACM Press, New York, NY, 83-92.
22. Norman, D. A. The Design of Everyday Things, 1988.
23. Spiekermann, S., J. Grossklags, and B. Berendt. 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In Proceedings of the Third ACM Conference on Electronic Commerce, Association for Computing Machinery (ACM EC'01), 38-47. New York: ACM Press.
24. Stiegler, M., Karp, A. H., Yee, K., Close, T., and Miller, M. S. 2006. Polaris: virus-safe computing for Windows XP. Commun. ACM 49, 9 (Sep. 2006), 83-88.
25. Trafton, J. G., E. M. Altmann, D. P. Brock, and F. E. Mintz. 2003. Preparing to resume an interrupted task: Effects of prospective goal encoding and retrospective rehearsal. International Journal of Human Computer Studies 58(4): 583–603.
26. Van Dantzich, M., R. Daniel, E. Horvitz, and M. Czerwinski. 2002. Scope: Providing awareness of multiple notifications at a glance. Proceedings of Advanced Visual Interfaces 2002, Trento, Italy.
27. Vila, T., R. Greenstadt, and D. Molnar. 2004. Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market. In Economics of Information Security. Vol 12 of Advances in Information Security, eds. L.J. Camp and S. Lewis, 143-154. Boston: Kluwer Academic Publishers.
28. Wayne R. Barnes, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance, 39 U.C. Davis L. Rev 1545 (2006)
29. Winn, J. Contracting Spyware by Contract, 20 Berkeley Tech. L.J. 1345 (2005)