Empirical studies on software notices to inform policy makers and usability designers

Jens Grossklags, Nathan Good

School of Information, University of California Berkeley,
102 South Hall, 94720 Berkeley, United States
{jensg, ngood}@ischool.berkeley.edu

This version: February 6, 2007

Keywords: HCI, privacy, security, legal issues, End User License Agreement, notice

1 Introduction

Human-Computer Interface (HCI) research is of increasing importance to security researchers as well as policy makers. As Internet access has become more prevalent, many issues that previously concerned only sophisticated technical users are now issues affecting the public at large. Issues surrounding digital privacy, copyright, electronic voting, notice & consent, and location-based systems are being pushed into the public policy arena because of advances in technology. Public policy advocates have traditionally accessed academic research as one means of understanding a problem, and HCI research provides a deeper understanding of the many technological issues discussed today. Indeed, many of the recent issues with new technologies have roots in problems that HCI has dealt with for years. For example, usability issues have caused security and privacy concerns for a broad range of issues such as electronic voting machines [Bederson et *al.*, 2003], the sharing of private personal information over P2P networks [Good and Krekelberg, 2003], phishing attacks [Dhamija et *al.*, 2006; Yee and Sitaker, 2006], and email message encryption [Whitten and Tygar, 1999].

Our research focuses on the primary means that security and privacy related information is currently communicated to the end user: the software notice and license agreements. We find software with potentially unwanted consequences and risks such as Spyware and Adware to be a particularly appealing field of study. We observe that in the marketplace millions of programs are installed bundled with advertisements and privacy-invading technologies [AOL/NCSA, 2004; Earthlink, 2005]. Many of these installations are made without any notice and consent procedures (e.g., through drive-by downloads), however, a surprisingly large number of programs are installed through deliberate user action and involving some form consent process. Users desire the functionality of programs they download, but frequently seem ill-informed about potential risks and negative consequences of installations. Indeed, the reason that spyware is difficult to accurately define is that the same piece of software may be considered unacceptable spyware by one user, an

acceptable trade for other services by another, or a valuable personalization system or notifier by a third. Because of this user-centered definition of what constitutes spyware, for some portion of software that meets the definition of spyware, it seems inappropriate to adopt an outright ban. Early efforts to combat spyware—much like anti-virus software efforts—measured their success based on how infrequently the software was installed. While such a measure can help provide security, it may also limit users' access to certain software combinations by denying them the opportunity to trade some privacy, speed, or attention for services or information they actually value. Imagine if your computer "protected" you by preventing you from ever transmitting your credit card information over the Internet; it would perhaps reduce your vulnerability to identity theft, but would at the same time deny you the benefits of shopping online. As response to usage restrictions due to security software (e.g., firewalls, anti-spyware) users might experience frustration. Left with their dissatisfaction users will often disable security technologies and, therefore, reduce overall security of the system.

In the case of spyware, it is not simply that the monitoring or notifications themselves may be valuable, but anecdotal evidence suggests [Delio, 2004], and our previous study confirms, that some users are willing to install spyware when the desired application with which it is bundled is of perceived high utility, and a comparable product without spyware is unavailable or unknown to the user [Good et *al.*, 2005]. In other words, at least in situations where users are unaware of other options, they are willing to give up some privacy, screenspace, or bandwidth as "payment" for an unrelated service or product they value. Accordingly, managing spyware requires that we engage the user in controlling their desktop instead of assuming we can simply do it for them.

We want to add that our works ties into an already existing public policy debate on balance of power between consumers and commercial entities. There has been a longstanding debate on the appropriateness of standard form contracts in business interactions with consumers. Already in 1943 a law review article criticized sellers for the harsh terms and conditions that are forced upon consumers in a take-it-or-leave-it fashion in many contracts [Kessler, 1943]. Many commentators have discussed the conflict of interests between the consumer and the business entity. On the one hand, businesses strive for monetary earnings but want to minimize potential liabilities out of transactions conducted in the marketplace. Accordingly, the typical vendor software license has much less to do with the licensing of technology than it does with the creation of multiple revenue streams flowing from the user to the vendor and the elimination or minimization of most forms of accountability from the vendor to the user [Overly and Kalyvas, 2004]. On the other hand, users want to benefit from the functionality of a program and other aspects that create hedonic and intangible values while limiting privacy, security and other risks of the interaction. Further, users want to reduce the effort involved in making sound decisions; standard form contracts help in an overwhelming number of situations to reduce transaction costs for businesses and consumers. In fact, it has been estimated that 99% of all commercial contracts are standard form contracts [Slawson, 1971].

Generally, economic forces should help to balance consumer desires and concerns with business interests. However, a recent research study supported the view that market conditions are generally uncorrelated with contract terms (for example, by

asking how price and market concentration determine the harshness of contract terms). The study also indicated that license terms on average provide less consumer protection than the Uniform Commercial Code baseline regulations [Marotta-Wurgler, 2005].

Despite this criticism it must be noted that standardization of contracts creates also many important benefits for consumers in the marketplace through cost reduction and allowing consumers to limit their attention to terms of the deal they particularly care about. End User License Agreements also serve as an important medium of communication between businesses and lawyers. However, in absence of simpler and more conspicuous modes of communication to the consumer (e.g., short notices [Good et al., 2007]) these agreements also serve as important information source for download and installation decisions. Our prior research suggests that users are often even uninformed about aspects of a program they genuinely are concerned about (such as pop-up advertisements and spyware). The result is unwanted installations of programs that are later regretted [Good et *al.*, 2005]. The current paper aims to explain this disconnect between consumer wishes and their market choices in more detail.

To this effect our research task is focused on evaluating the readability and usability of End User License Agreements (EULAs) that represent the legal state of the art of informing users and obtaining user consent. We present preliminary results from an empirical study of 50 popular consumer programs on the accessibility and readability of the associated EULAs. We also briefly discuss results from a user study involving 64 users in program installation tasks. Users were observed during their interaction with an experimental program installation environment. We recorded their reading behavior, decisions to complete or cancel an installation and their responses to post-experimental surveys.

Both studies are significant extensions of our prior work [Good et *al.*, 2005]. On the one hand, we discussed in our first paper the readability metrics of only 5 programs that we randomly selected. The current study gives a more thorough overview of the notice of consent practices for an important sample of 50 consumer programs that are the most popular freeware/shareware or free-to-test versions across multiple functional categories. On the other hand, we also conducted a more thorough experimental analysis. In Good et *al.* [2005] we reported results of an in-depth user study on notices with a small sample set of 30 users across three experimental conditions. Many questions were left open and in need of further experimentation to determine or substantiate results. In this paper we will only be able to cover initial results from the new study due to space limitations but want to give the reader sufficient insights on the current experiment and the results.

Our goal is to facilitate interdisciplinary research on informed consent, and facilitate the creation of usable law based on usable technologies. The emergence of location-based systems, camera phones, RFID & sensor networks demand further research on how to better notify consumers about their privacy rights. In an increasingly networked society, new technologies and methods of distributing media raise issues regarding how content providers and consumers view ownership of digital content. Efforts to understand these complexities and inform security researchers as well as policy makers could benefit directly from participation of HCI practitioners as well as from prior research in this area.

2 Empirical study of End User License Agreements

As the data set, we chose Download.com's top 50 most downloaded software programs[1]. Download.com is a leading source for primarily free or free-to-try consumer software downloads covering major software vendors as well as small distributors but the program offerings are not necessarily representative of all consumer programs available.[2]

Related to our study Kucera et al. [2005] reported on the prevalence of spyware in a similar sample of download.com's most popular programs.[3] When defining spyware narrowly as programs that surreptitiously collect personal information from computers linked to the Internet the authors confirmed the existence of spyware for three of those programs. The current policy of the distributor does not allow for software including viruses or spyware[4], however, the website does not clearly define these terms.

Recently, the Anti-Spyware Coalition formulated a broader characterization of spyware (and other potentially unwanted software).[5] Their definition includes technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.

Our focus in this study is on analyzing the readability of license terms distributed with typical software available to consumers. We defer the content analysis of these agreements and a technical analysis to later stages of our research. It is to be expected that many of the terms are unremarkable and of little concern to the user [Schechter, 2000]. However, we note that our preliminary analysis suggests that the programs included in our sample included terms (including privacy implications, restrictions of usage and legal rights, distribution of adware) that are likely to the detriment of many consumers and may overlap with a broader definition of spyware.

The software programs were grouped by the category and subcategory types given by Download.com: Internet (26%), Audio & Video (22%), Security & Anti-Spyware (20%), Games (10%), Utilities (10%), Design & Photo (2%), Desktop Enhancements (2%), Developer Tools (2%), and Networking (2%).

---

[1] We chose the Top 50 most downloaded software programs for the week ending April 9, 2006.

[2] They report to serve "over 27,000 publishers representing 35,000 products and 132 countries around the world, our product library generates over 2.3 million downloads each day." http://www.upload.com/1200-21_5-5139590.html, visited February 5, 2007.

[3] Kucera et *al.* obtained data for the week ending January 12, 2003.

[4] See, for example, http://www.upload.com/1200-21_5-5081541.html?tag=fd, visited February 5, 2007.

[5] http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm

2.1 Timing and Presentation of the End User License Agreement presentation to the user

For each software program, we initiated the downloading and installation process, and stopped the process at the point where we encountered a EULA. We copied the EULA that appeared on-screen and canceled the download at this point, and thus did not capture any additional terms that may have been presented to the user after this point. If we did not encounter a EULA during the installation process or after program installation we expanded the search to the distributors' website. See Figure 1 for a typical display situation of a EULA during the installation process.

We observed that the terms were presented at different stages during the installation process for different programs: e.g., before the installation had begun or after the installation process. Knight Online 1.299 showcased a so-called "first-run notice"[6] that occurs the first time a (or potentially each) user starts the program.

Common sense regarding notice and consent would dictate that information to users should be provided before an installation is initiated or completed. In research reported elsewhere we investigate the impact of the timing of notices more thoroughly [Good et *al.*, 2007].

More problematic from an accessibility standpoint is the omission of notice during the installation process. Adobe Reader and Irfan View, had EULAs only on their websites. It is doubtful whether users would search for these terms if not included in the installation dialog. One further significant difference appeared between the two programs. Irfan View's installer was directly accessible at download.com's website. Users interested in Acrobat were redirected to Adobe to initiate download[7]. Under the 'download' button on Adobe's site the EULA was accessible by clicking on a link "By downloading software from the Adobe web site, you agree to the terms of our license agreements […]".

Software providers differ in the type of notice and presentation of notice they provide to the user. From a legal perspective these installation scenarios introduce different challenges and likely impose different consequences on the user. For example, courts have started to differentiate between different modes of presentation of notice when they decide whether a user is bound by terms. See, for example, Casamiquela [2002] who discusses caselaw and legal theory on browsewrap versus clickwrap agreements[8].

---

[6] A recent report by Microsoft [Microsoft, 2006] distinguishes between Just-In-Time, First Run, Installation Time, and Out-of-The-Box notices. Out-of-the-Box notices were not observable from our download.com sample. We did not test for Just-In-Time notices that occur in the moment before sensitive data is transmitted or some other potentially harmful or unwanted action is undertaken by the program. The majority of the programs featured Installation Time notices.

[7] We expect that many users have access to Adobe Acrobat's installation file also without visiting Adobe's website.

[8] Clickwrap agreements include situations in which a software vendor requires users to click "I agree" or similar buttons or click-check radio buttons or boxes to signify consent. A license is likely to be characterized as browsewrap if only a link to the terms is available to the user instead of the complete license.

We were unable to locate a license agreement for Limewire, Limewire (Mac), and Morpheus on the respective company websites or during the installation. There is anecdotal evidence that file-sharing companies refrain from using EULAs in an effort to limit possible liability for contributory infringement, as the presence of a license agreement would establish an ongoing relationship with the customer.

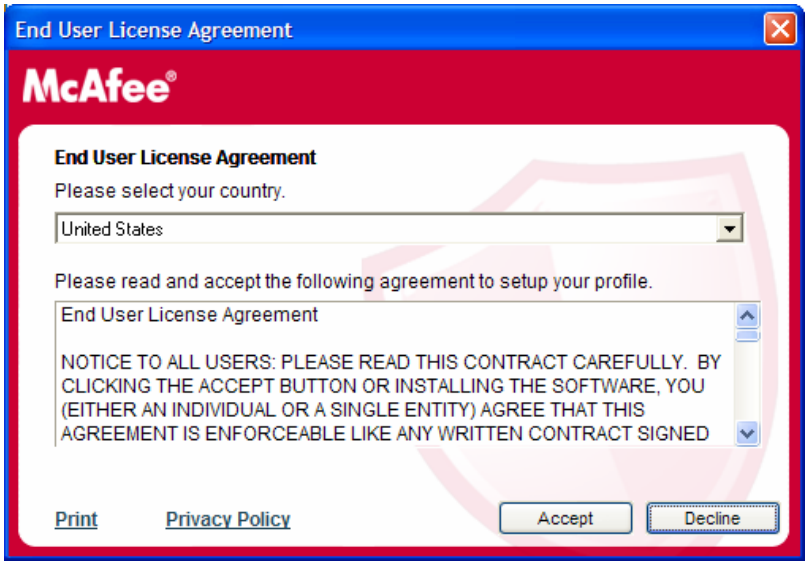

Figure 1 End User License Agreement presentation during installation (McAfee AntiVirus vso_10027_en-us-30day)

While the typical presentation of a EULA follows the pattern observable in Figure 1 access to the agreement is not always obvious. For example, the installation dialogue displayed in Figure 2 only links to the read me file that, however, contains a contractual document.[9] We believe that this access regime is from a user point of view totally unexpected.

EULAs were often presented in a format that limits users in gaining a quick overview over the terms covered. For example, the notice screen displayed in Figure 1 allows the user to only review about 50 words at a time without scrolling. The complete notice, however, is 5500 words long.

[9] Excerpt from readme file: "THIS SOFTWARE IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WHICH ARE HEREBY DISCLAIMED. […]"

Figure 2 Need for Speed Most Wanted PC demo installation dialogue

2.2 Length of EULAs

For the software programs which had EULAs, the average EULA length was 2752 words (std. dev. = 2228.8), corresponding to about 11 pages of double-spaced text (see Figure 3). Assuming that the reading difficulty of the EULA is average as reported in psychology research, the average reading time for the EULA is about 13 minutes[10]. The shortest EULA (Little Fighter) was 111 words, the longest (Adobe Reader) was 9313 words, corresponding to approximately 41 pages of double spaced text and an average reading time of 47 minutes. It is likely that the length of time it will take an average consumer to *understand* the EULA is even longer than 47 minutes.

Practically, the average EULA is even longer than what is shown in Figure 3. Many of the EULAs have website links to additional information and terms that are incorporated into the EULA, such as Terms of Use, Terms of Service, Privacy Policies, and third party EULAs. For this study we did not review any of these additional linked documents. Further, to fully understand what they were agreeing to, the user would also have to research various statutes and rules that are mentioned within the text of the EULAs, such as the "Commercial Arbitration Rules of the American Arbitration Association". In one particularly egregious example, Good et *al.* [2003] evaluated a KaZaA EULA, and noted that it contained 17458 words in the

[10] Assuming an average reading rate of 200 words/minute. Lewandowski et *al.* [2003] found an average reading rate for college students of 189 words/minute when subjects were given oral reading probes measuring words read correctly per minute (WRCM). Younger students and elderly citizens will likely read and comprehend slower on average. One reviewer correctly observed that it would be advisable to measure reading speeds specifically for EULAs. We have so far not conducted the required experiment.

EULA itself, 4 hyperlinks to outside sites and policies, 78 locations of third parties and policies, and 5 opt-out options, and would take an average reader approximately 88 minutes to read.

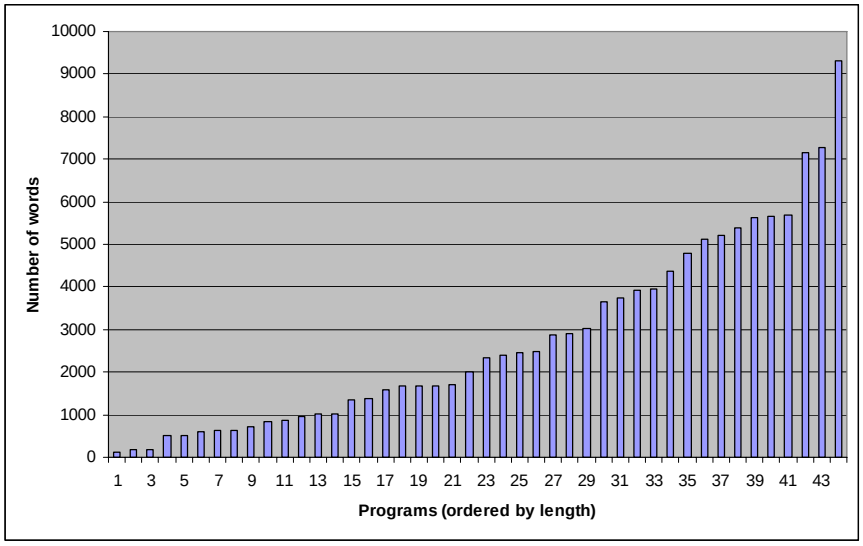

Figure 3 Length of End User License Agreements

2.3 Simple readability measures

We analyzed Flesch-Kincaid Reading Level [Kincaid et *al.*, 1975], and Flesch Reading Ease levels [Flesch, 1948] for the EULAs in the program sample. The Flesch-Kincaid Reading Level uses average sentence length and average number of syllables per word to give a rough measure[11] of a document's readability. The scores range from 1.0 to 12.0, corresponding to the reading level of an average student in grades 1 through 12, respectively. The scores do not go higher than 12.0, and thus the Flesch-Kincaid Reading Level cannot provide information as to whether the reading level is actually higher than a 12th grade reading level. 63% of the EULAs scored 12.0, the highest score possible. The average score was 11.2 (std. dev. = 1.6), with scores ranging from 5.7 to 12.0. Because the scores cannot go higher than 12.0, and

[11] One critic of the Flesch-Kincaid models noted that "to measure readability, coherence and comprehensiveness of a text, more than surface features need to be taken in consideration than surface features alone. Quantitative and qualitative factors like the number of anaphora, number of overlapping text segment, vocabulary difficulty, sentence and text structure, concreteness and abstractness, are equally needed. It is the sum of these and other factors that constitutes cohesion." University of Memphis Institute of Education Sciences, http://cohmetrix.memphis.edu/cohmetrixpr/readability.html , visited on May 11, 2006.

because of the large percentage of EULAs with the maximum score, the average score of 11.3 is likely skewed lower than it should be.

The Flesch Reading Ease also uses average sentence length and average number of syllables per word to give a rough measure of a document's readability. The Reading Ease scoring scale ranges from 0 to 100, with a higher score corresponding to easier reading ease.

As a rule of thumb, scores of 90-100 are considered easily understandable by an average 5th grader. 8th and 9th grade students could easily understand passages with a score of 60-70, and passages with results of 0-30 are best understood by college graduates. *Reader's Digest* magazine has a readability index of about 65, Time magazine scores about 52, and the Harvard Law Review has a general readability score in the low 30s. This test has become a U.S. governmental standard. Many government agencies require documents of forms to meet specific readability levels. Most states require insurance forms to score 40-50 on the test.

The average Reading Ease score was 35.7 (std. dev. = 10.7), with a low of 18.5 (WinZip), and a high of 69.8 (Mario Forever). Fully 89% of the EULAs scored under 50, and only 1 EULA (Mario Forever) scored in the ideal range when for writing for the general population (60-70)[12]. As no EULA scored at either extreme end of the range, the Reading Ease score is likely a better measure of readability than the Reading Level score.

Readability studies were conducted for the domain of privacy notices. Jensen and Potts [2004] found an average reading ease of 34.2 for popular entertainment websites and 36.5 for health care sites. Breese and Burman [2005] found a reading ease of 42.2 for privacy practices of 185 institutions listed in the 2004 US News & World Report's 'best hospitals' issue. Hochhauser [2001] found an average reading ease of 34 for 60 financial privacy notices (and a level of 39 for 31 HIPAA notices [Hochhauser, 2003]).

2.4 Discussion

If privacy or security risks are disclosed in the EULA then the length and reading ease will directly impact users' comprehension and decision making. However, if consumers cannot understand the terms to which they are ostensibly agreeing, have they really formed a valid contract with the company, or do they have a duty to read?

It appears that the EULAs in our sample are characterized by sizable length and low readability. Additionally, they are hampered by user interface issues that make it hard for users to find and access the EULAs and/or attain a quick overview over important terms.

Hochhauser [2001] suggests that several language and presentation modifications can be undertaken to improve readability and understanding. For example, the use of active everyday language, short explanatory sentences in bulleted lists, avoiding imprecise language including double negatives and effective highlighting of important terms can contribute to reader's improved decision making.

---

[12] *See e.g.*, http://www.diabetesvoice.org/issues/2004-09/Diabetes-related_websites_are_they_readable.pdf.

But grammatical simplification of contracts will not solve all comprehension problems. Research by, for example, Masson and Waldron [1994] demonstrates that the success of simplification of sentence structure etc. is hampered through the complexity of the legal concepts that are at the heart of online notices. Not only legal concepts are hard to understand. Acquisti and Grossklags [2005] discuss consumers' limited knowledge and understanding of privacy and security risks. Further, misaligned economic incentives limit distributors' desire to improve EULA terms (see, for example, Vila et al. [2004]).

EULAs are often written from lawyers for lawyers. However, in absence of better information sources consumers have to rely on them to make successful a priori choices about software programs that are often difficult to uninstall and might significantly impact security, privacy, usage rights and performance.

Some commentators have discussed the role of experts, consumer advocates and user-to-user recommendations as a tool to improve decision making. For example, Hillman [2006] argues that mandatory display of license terms on Web sites will improve access of consumer protection organizations. However, he cautions that the improved accessibility might backfire (at consumer rights) if terms still do not receive added scrutiny, or are not read more often compared to the current notice regime. Download.com alone distributes 35000 programs - it appears unlikely that even all somewhat popular programs do receive enough scrutiny.

In future work we aim to more closely research interface aspects of EULA presentation to the user. We are also interested in analyzing the contents of these agreements to a greater extent.

3 Experiment

Below we report survey results and basic reading time measures observed in the experimental part of the project.

3.1 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.

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. 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. 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. Users were given a user id, which was matched up against a list of acceptable identifiers and associated with a treatment and a program ordering.

A representation of the framework architecture is presented in Figure 4.

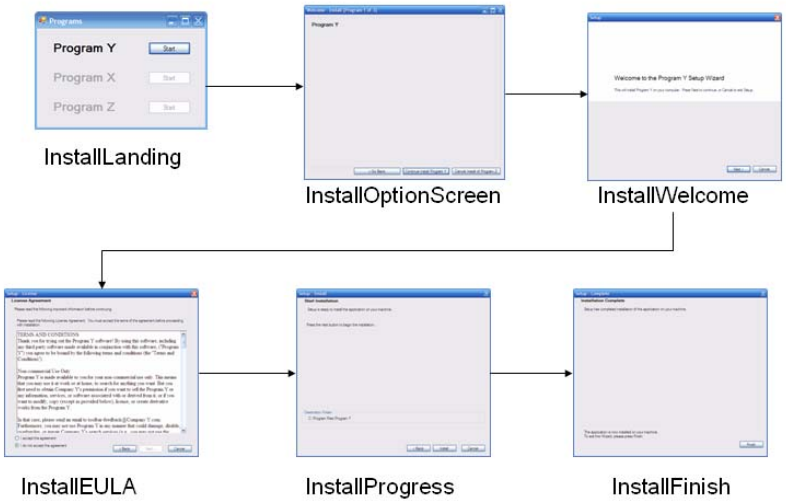

Figure 4 Framework architecture of experiment

We selected popular consumer programs from our previous study [Good et *al.*, 2003] 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 experimental program titles and descriptions are listed below:

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

We also replaced the brand names and other identifying information in the EULA statements with the above generic titles. The ordering of the programs was randomized within the subject pool.

All three programs vendors disclose in the End User License Agreements that they take significant influence on the user's desktop experience. They differ in the disclosed impact on privacy and security. Some aspects of these programs fall within the broader definition of spyware and adware.

3.2 Subjects

64 subjects participated in the treatment that we discuss below[13]. Subjects were paid $20 for their participation, and were recruited by a university service with access to a subject pool of several thousand students.

On average we had a young and very computer-experienced group of users. For example, More than 80% stated that they maintained their home computer themselves.

3.3 Survey results

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.

Supporting these results, Jensen and Potts [2004] report that for a university service standalone website requiring registration only 0.24% of over 50000 users visited the site's privacy policy. Another software provider reported from an experiment in which a $1000 cash prize was offered in the EULA that was displayed during each software installation, yet the prize was only claimed after 4 months and 3,000 downloads of the software [PC Pitstop].

In contrast to EULA statements, food labels and credit card statements have been subject to substantial standardization and simplification. However, complete information about food ingredients and consequences of signing up for a new credit card are difficult to present to the user in a unified format and labels always need to be selective. Different states take different approaches towards what warnings and information are useful for consumers in their decision making. Similarly, consumer perceptions and reading behavior varies widely across the population. Individuals' health concerns are a strong driver for reading behavior. For example, Kreuter et *al.* [1997] found that patients with high blood pressure searched labels for sodium information, however, did not investigate other ingredients more often than the rest of the population.

With respect to software installations the presence of individual differences in reading behavior and other behaviors suggests that personalized solutions have promise. Analogously, consumers with certain allergies are insufficiently supported by many current food labels. Some Web users might be well-served by the current notice and EULA 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. We also note that a state-by-state approach is unworkable for

[13] Until now we have completed three laboratory experiments with a total of 240 users. Different results of these experiments are reported in Good et *al.* [2007] in which we focus on short notices and the timing of notice presentation to the user (see this paper for more details on the user population and experimental setup).

program downloads from the Internet. Therefore, enforcement action will likely be needed from the federal government or agencies such as the FTC.

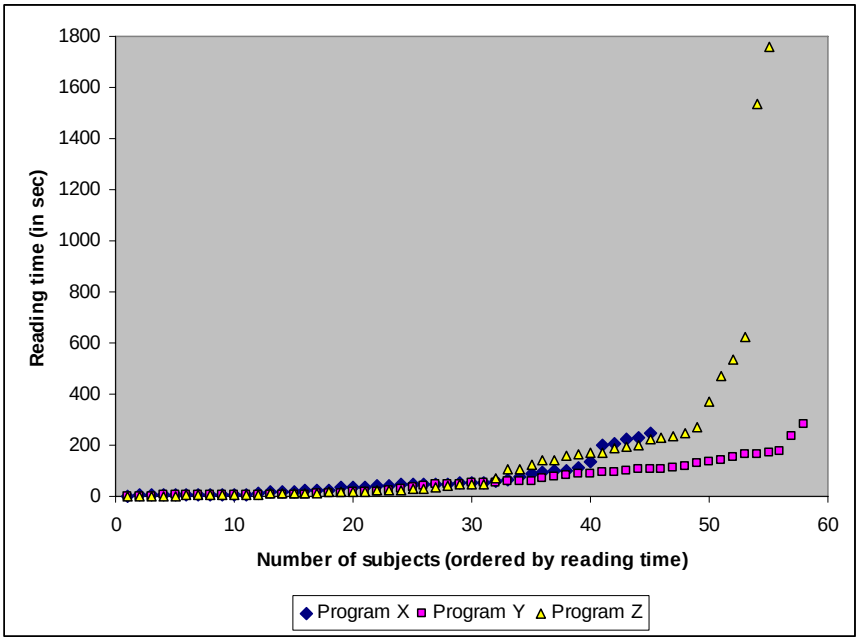

Figure 5 Reading time for End User License Agreement Screen for the three different programs (in sec)

3.4 Reading behavior in the experiment

In this paper we report data for individuals that installed programs X, Y, and/or Z leaving us with 45, 58, 55 observations for the respective programs.[14] On average individuals resided on the screen that showed the complete End User License Agreement in a scrollbox for one or two minutes (Program X: 59.7 sec, 66.4 std.dev.; Program Y: 64.9 sec, 64.4 std.dev.; Program Z (with outliers): 162.6 sec; 323 std.dev.; Program Z (without 2 outliers): 106.6 sec, 141.0 std.dev.). More than 55% of the experimental subjects spent less than one minute on this screen. Only 3.7% deliberate on this screen for more than 5 minutes. It appears the installation of the filesharing program Z caused more individuals to slow down in their reading behavior. We plotted the reading times for the three different programs in Figure 5. The time

[14] Subjects that canceled installation did not always progress through the installation routine until they were able to review the EULA.

required to pass through the EULAs is 14 min, 10 min, 14 min for Program X, Y, and Z, respectively.[15]

We were also interested in the time individuals spent on the EULA screen in comparison to the other parts of the installation dialogue. Since this screen was the only one that contained important information about the program we would expect the ratio between the two measures to be below one. The other screens prompted individuals to merely click to continue.

Up to 32.8% of the users spent more time clicking through screen without important information resided compared to the EULA screen (Program X: 71.1%; Program Y: 67.2%; 74.5%).[16]

3.5 Discussion

The results serve as a benchmark for reading behavior if individuals are unaffected by brand recognition, message framing and sophisticated user interface design techniques. It is not a reading speed test. Rather the study provides insight into the distribution of reading times across a reasonably-sized subject group in a controlled laboratory context. Surprisingly, even without particular knowledge about the programs' terms concerning privacy, security and usage rights and without time pressure almost no subjects spend enough time on the EULA screen to pass through the notice agreement. In contrast, Hillman [2004] reported that one third of the law student respondents to his survey would more likely read notices if the vendor is unknown.

Well-known limitations of laboratory studies apply also to our experiment. We cannot prove that individuals would behave exactly in the same way outside of the laboratory, but we expect similar behavior. Our subject pool consisted mainly out of young and computer-literate college students. We believe them to be a natural target audience for the type of programs in the study. Other demographical groups are likely to demonstrate slightly different behaviors, for example, older people often report higher privacy concern and might act accordingly.

We have already hinted at several reasons for the absence of careful reading. Notices are often impenetrable, written in legalese, too long. Further many consumers do not expect them to contain useful information that helps them to make better decisions [Good et al., 2005]. Consumers feel that it is not worth it to read notices [Hillman, 2006; Vila et *al.*, 2004].

---

[15] Again, using an average reading speed of 200 words/minute [Lewandowski, 2003].

[16] This cut-off level is somewhat arbitrary, but we posit that the reading time on the EULA screen should be, in general, a multiple of the time spent on basically content-free screens that merely state a generic program name and progress of the installation process.

4. Conclusion

We have presented results on readability and presentation of EULAs from 50 popular free or free-to-try programs available for download on a distribution page. We suggest that the length and complexity of documents can significantly lower the notice and consent success rate achieved.[17] According to readability expert Mark Hochhauser [2003], the length of legal documents often creates information overload leading to increased stress, impaired judgment and helplessness. This effect is particularly strong for older readers. Moreover, rewriting these documents in simple language is often impossible [Hochhauser, 2003] and the underlying legal concepts might still be too hard to understand for interested readers [Masson and Waldron, 1994]. All these effects appear particularly strong in EULAs since their length and the range of issues covered in them is beyond, for example, Web privacy notices. We suggested in public FTC hearings that federal authorities should revisit their basic approach to benchmarks with respect to industry self-regulation to create reliable standards for consumers to rely upon [Turow et al., 2006].

We also observed different presentation styles and timing of notice display. This is an additional source of confusion to Web users who will not expect to find important legal information, for example, only on the company's Web site or buried in a read me file. In our current work we are particularly interested in the influence of different but conspicuous timing modes. In treatments not discussed in this paper we explicitly modified the notice experience for the user so that especially designed short notices would appear either at the start or the end of the installation dialogue in addition to the long-form EULA [Good et *al.*, 2007].

Without significant improvements to notice and consent procedures for consumer programs it is doubtful that most consumers genuinely assent to the use of their desktops for advertisements, the installation of software with behavior that falls within the broad definition of spyware, or limitation of usage rights. We do not expect that there exists a one-size-fits-all solution, in particular, given the increasing popularity of mobile and small-screen devices. Notice and consent involves many stakeholders. Companies are urged to improve their information dissemination practices and regulation may carefully adjust misaligned incentives in the market place. But improved notice procedure will likely result also in a more substantive obligation for users to read notices.

Acknowledgements

We are greatly indebted to Susheel Daswani for constructing the experimental framework. Part of this work is conducted jointly with Joe Konstan, Deirdre Mulligan and Becca Shortle. We also thank Chris J. Hoofnagle, Ira Rubenstein and the anonymous reviewers for their valuable feedback and suggestions. Jens Grossklags' work is supported in part by the National Science Foundation under ITR award ANI-0331659.

This work was also supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations:

[17] This also includes an informed decision not to install a particular program.

AFOSR (#FA9550-06-1-0244) Cisco, British Telecom, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies.

References

1. Acquisti, A. and Grossklags, J.: Privacy and Rationality in Individual Decision Making,. IEEE Security and Privacy, Vol. 3, No. 1, January/February (2005) 26-33.
2. AOL and National Cyber Security Alliance: AOL/NCSA online safety study, (October 2004). http://www.security.iia.net.au/downloads/safety_study_v04.pdf
3. Bederson, B.B., Lee, B., Sherman, R.M., Herrnson, P.S., and Niemi, R.G.: Electronic voting system usability issues. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2003) 145 – 152.
4. Breese, P., Burman, W.: Readability of Notice of Privacy Forms Used by Major Health Care Institutions. Journal of the American Medical Association 293 (2005) 1593-1594.
5. Casamiquela, R.J.: Contractual Assent and Enforceability in Cyberspace. 17 Berkeley Tech. L.J. (2002) 475-495.
6. Delio, M. (2004) "Spyware on My Machine? So What?" Wired News, December 06, 2004. Available at: :http://www.wired.com/news/technology/0,1282,65906,00.html
7. Dhamija, R., Tygar, J.D., and Hearst, M.: Why Phishing Works. Proceedings of the SIGCHI conference on Human factors in computing systems (2006) 581 - 590.
8. Earthlink: Earthlink spy audit: Results complied from Webroot's and Earthlink's Spy Audit programs (2005). http://www.earthlink.net/spyaudit/press.
9. Flesch, R.: A new readability yardstick. Journal of Applied Psychology, 32 (1948) 221-233.
10. Good, N., and Krekelberg, A.: Usability and privacy: a study of Kazaa P2P file-sharing. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2003) 137 – 144.
11. Good, N., Dhamija, R., Grossklags, J., Aronovitz, S., Thaw, D., Mulligan, D., and Konstan, J.: Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. Proceedings of the Symposium On Usable Privacy and Security (SOUPS 2005), Pittsburgh, PA, July 6-8 (2005) 43-52.
12. Good, N., Grossklags, J., Mulligan, D., and Konstan, J.: Noticing Notice: A large-scale experiment on the timing of software license agreements, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2007), San Jose, CA, April 28 - May 3 (2007).
13. Hillman, R.A.: Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire. 104 Mich. L. Rev. (2006) 837-856.
14. Hochhauser, M.: Compliance v Communication. Clarity: Journal of the International Movement to simplify legal language, Vol. 50 (November 2003) 11-19.
15. Hochhauser, M.: Readability of HIPAA Privacy Notices (2003). Available at: http://benefitslink.com/articles/hipaareadability.pdf
16. Hochhauser, M.: Lost in the Fine Print: Readability of Financial Privacy Notices (2001). Available at: http://www.privacyrights.org/ar/GLB-Reading.htm
17. Jensen, C., and Potts, C.: 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 (2004) 471–78. New York: Association for Computing Machinery.
18. Kessler, F.: Contracts of Adhesion – Some Thoughts About Freedom of Contract. 43 Columbia Law Review (1943) 629.

19. Kincaid, J., Fishburn, R. Jr., Rogers, R., and Chissom, B.: Derivation of New Readability Formulas for Navy Enlisted Personnel. CNTECHTRA Research Branch Report (1975) 8-75.
20. Kreuter, M.W., Brennan, L.K., Scharff, D.P., and Lukwago, S.N.: Do nutrition label readers eat healthier diets? Behavioral correlates of adults' use of food labels. American Journal of Preventive Medicine, Vol. 13, No. 4 (1997 Jul-Aug) 277-83.
21. Kucera, K., Plaisent, M., Bernard, P., and Maguiraga, L.: An empirical investigation of the prevalence of spyware in internet shareware and freeware distributions. Journal of Enterprise Information Management, Vol. 18, No. 6 (2005) 697 – 708.
22. Lewandowski, L.J., Codding, R.S., Kleinmann, A.E., and Tucker, K.L.: Assessment of Reading Rate in Postsecondary Students. Journal of Psychoeducational Assessment, Vol. 21, No. 2 (2003) 134-144.
23. Marotta-Wurgler, F.: Competition and the quality of standard form contracts: An empirical analysis of software license agreements. New York University working paper (2005).
24. Masson, M.E.J., and Waldron, M.A., Comprehension of legal contracts by non-experts: Effectiveness of plain language redrafting, Applied Cognitive Psychology, 8 (1994) 67-85.
25. Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services. (October 10, 2006).
26. Overly, M., and Kalyvas, J.R.: Software Agreements Line by Line: A Detailed Look at Software Contracts and Licenses & How to Change Them to Fit Your Needs. Aspatore Books (2004).
27. PC Pitstop (2005) "It pays to read EULAs." Available at http://www.pcpitstop.com/spycheck/eula.asp (last accessed February 5, 2007)
28. Schechter, R.E.: The Unfairness of Click-On Software Licenses. 46 Wayne L. Rev. (2000) 1735-1803.
29. Slawson, W.D.: Standard Form Contracts and Democratic Control of Law Making Power. 84 Harvard Law Review (1971) 529-566.
30. Turow, J., Hoofnagle, C., Mulligan, D., Good, N., and Grossklags, J. (2006) Consumers & Privacy In the Coming Decade, Session on Communicating with Consumers in the Next Tech-ade - The Impact of Demographics and Shifting Consumer Attitudes, Public Hearings on Protecting Consumers in the Next Tech-ade, Federal Trade Commission, Washington D.C., November 6 - 8, 2006.
31. Vila, T., Greenstadt, R., and Molnar, D.: Why We Can't Be Bothered To Read Privacy Policies: Models of Privacy Economics as a Lemons Market. In Economics of Information Security, L. J. Camp and S. Lewis (Eds.), Springer-Verlag (2004) 143-153.
32. Whitten, A. and Tygar, J.D.: Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium (1999) 169 -- 184.
33. Yee, K.-P., and Sitaker, K.: Passpet: Convenient Password Management and Phishing Protection. In Proceedings of the Symposium on Usable Privacy and Security (2006) 32 – 43.