Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices

By: Masooda Bashir, Kevin A. Hoff, Carol M. Hayes, and Jay P. Kesan
University of Illinois at Urbana-Champaign
Urbana, IL 61820

Introduction

The current approach to digital privacy in the United States does not facilitate informed consumer decision-making. In fact, the existing "notice and choice" approach often encourages *blind consent*, in that consumers frequently consent to privacy policies and terms of service agreements without actually knowing the significance of the terms to which they are consenting. A major source of the problem is that consumers have neither the time nor the energy required to read all of the textual notices they encounter on a day-to-day basis (McDonald & Cranor, 2008). In addition, consumers often do not have a valid alternative to accepting a website's privacy policy. This lack of choice reinforces the ineffectiveness of notices, because in the absence of meaningful choice, consumers are likely to think that learning about a website's privacy policy is futile.

A recent survey we conducted suggests that a lack of consumer background knowledge may also contribute to the problem. A more effective "notice and choice" approach to digital privacy should therefore emphasize consumer knowledge in addition to providing meaningful choices. If consumers remain under-informed, the effectiveness of any future approach will be limited. Thus, in this position paper, we propose a new instrumentality for improving the effectiveness of notices: *Knowledge-based Individualized Privacy Plans* (KIPPs). The basic goal of KIPPs would be to promote greater comprehension of the significance of privacy notices by altering the framing, presentation, structure, and /or language of notices to better accommodate the needs of individuals with varying degrees of background knowledge. By increasing comprehension, KIPPs could increase the capabilities of consumers to base their website usage decisions on the privacy practices of different companies.

Background

The idea of privacy has evolved with technology. Modern scholars such as Daniel Solove have emphasized the role of information technology in changing the foundational dynamics of effective privacy law (Solove, 2006). The plethora of websites and other services that collect and process personal information in today's society makes it nearly impossible for individual consumers to remain informed of how their personal information is being handled by different companies. Lorrie Cranor has discussed and evaluated standardized alternatives to textual privacy policies, including privacy nutrition labels and icons (Cranor, 2012). Other researchers, such as Helen Nissenbaum, have discussed the current discrepancy between what people say they want in terms of privacy and what people actually do (Nissenbaum, 2009). This so-called privacy paradox may be partially caused by a lack of consumer understanding with respect to the importance of privacy notices and the choices available to individual consumers.

In order to evaluate the extent to which comprehension gaps might contribute to this privacy paradox, we recently conducted a two-part online survey centered around consumer knowledge and opinions. The survey link was distributed primarily through email at the University of Illinois at Urbana-Champaign. We collected about 500 responses for each part of the survey, with the majority of responses coming from individuals between the ages of 18 and 25. Figure 1 below displays the results of a broad opinion-based question regarding the extent to which privacy notices influence online behavior. Only 43% of respondents indicated that they had ever refused to use a website strictly because of the website's privacy policy or terms of service agreement. This provides further evidence that privacy notices do not usually influence consumer behavior.

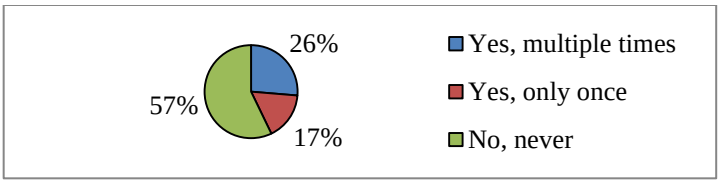

Figure 1. Survey responses to, "Have you ever decided not to use a website strictly because of the website's Privacy Policy or Terms of Service agreement?" (n=707)

In addition to the opinions, we also conducted an extensive evaluation of online privacy knowledge. Past research has yet to address this topic in much detail so our survey offers substantial new insight. Table 1 below reports the percentage of respondents who correctly answered certain questions in the survey. Note that the research questions displayed in the table are condensed versions of the actual questions from the survey.

TABLE I. PERCENTAGE OF CORRECT RESPONSES TO KNOWLEDGE-BASED SURVEY QUESTIONS (N=455)

Research Question	**Percentage of Respondents who Answered Correctly**
Are online advertising companies required by law to ask for users' permission before tracking their online activity?	68%
Can online advertising companies use the emails sent and received on free webmail services to develop targeted advertisements?	67%
Do free websites, such as Facebook and Google, make money by selling user information directly to marketing companies?	56%
Does tweeting a status update on Twitter constitute the use of cloud computing?	41%

The response patterns above highlight several important areas where consumer comprehension appears inadequate. For example, about 33% of respondents were unaware that online advertising companies could use emails sent and received on free webmail services to develop targeted advertisements. Additionally, about 44% of respondents did not know that free websites could profit by selling user information directly to marketing companies. These knowledge gaps are striking given the fact that our survey was distributed online and about 29% of our respondents had a graduate level degree (which is almost three times the national average; United States Census, 2009). If close to one half of our respondents were unaware of one of the main methods used by free websites to make money, it is likely that many millions of Americans are similarly uninformed.

Although most of the questions from our knowledge survey did not ask about the privacy notices of individual companies, they explored pertinent background knowledge. When individuals lack such knowledge, the information within privacy notices might seem irrelevant or confusing, which would probably deter individuals away from reading privacy notices. For example, the 59% of our respondents who were unaware of the fact that tweeting a status update on Twitter constitutes the use of cloud computing might be less inclined to read Twitter's privacy policy compared to more informed individuals. Thus, in order to promote readership and understanding of privacy notices for individuals with varying degrees of background knowledge, we propose Knowledge-based Individualized Privacy Plans (KIPPs).

Knowledge-based Individualized Privacy Plans (KIPPs)

Sufficient consumer knowledge is one of the most important antecedents of an effective "notice and choice" approach to digital privacy. As it stands today, the excessive length, complexity, and technicality of many privacy notices make the notices appear almost impenetrable to the average person. In order to fully understand most notices, readers must possess a certain degree of background knowledge

which, based on the results of our survey, is likely deficient for many millions of people. Thus, by addressing certain crucial gaps in preexisting knowledge, KIPPs could promote increased readership rates and subsequently enhance the role of privacy notices in informing consumer decision-making.

The widespread diversity of people who use information technology across the United States and elsewhere makes a "one-size-fits-all" approach impractical. Personalizing the presentation and structure of information for diverse individuals has been successful in other domains. For example, Individualized Education Programs (IEPs) are widely used in schools across the United States to help students with varying abilities improve their educational outcomes. In developing IEPs, teachers team with parents and other individuals to identify the unique needs of a student through an evaluation process. Once a student's needs are identified, IEP team members construct an individualized plan for the student and subsequently reevaluate the plan based on the student's progress (U.S. Department of Education, 2006).

The overall goal of Knowledge-based Individualized Privacy Plans (KIPPs) would be quite similar. Individuals' privacy knowledge would be assessed and a personalized privacy plan could be generated based on the results. The evaluation process could either be subjective (i.e., asking the user to rate his or her privacy knowledge) or objective (i.e., having the user answer knowledge-based questions), depending on a user's preferences and the practicality of each approach in a given context. Regardless of form, however, the assessment would need to be brief and carefully constructed in order to be useful on a large-scale. Effective questions could assess knowledge regarding the data trade for personal information online, the alternatives to using a service, and the privacy protections available to consumers.

Once the evaluation process is completed, the results would be used to form the basis of a KIPP. The degree of specificity versus generality for KIPPs could vary for diverse users in distinct contexts. KIPPs could be as simple as highlighting the importance of privacy notices for users who are unaware of the techniques commonly used by websites to collect, process, and distribute personal information. They could also be more complex by aiding users in more efficiently skimming privacy notices for key terms and provisions, or by helping users compare the privacy practices of different companies. These details and other implementation issues would likely depend on the goals of individual users and the entities who provide KIPPs.

Implementation Challenges

In order to be effective in practice, KIPPs would need to address the incentives of consumers, businesses, and third-parties alike. Thus, as a starting place, one might ask, "Why would companies or third parties want to provide users with KIPPs?". Our response depends on whether KIPPs are offered on a company-to-company basis or on a broader scale, encompassing the privacy notices of multiple companies within a given domain. If the former approach is used, companies would likely provide KIPPs to help users interpret their own privacy notices. Companies might be interested in using KIPPs in order to improve customer relations, increase transparency, and/or compete with market alternatives. If the latter approach is used and KIPPs are implemented using a broader approach, they would likely need to be provided by a third-party, such as a privacy advocacy group or industry-wide committee. The third party organization could set forth general guidelines for structuring privacy notices to accommodate consumers with varying degrees of preexisting knowledge. If the guidelines proved effective and gained popularity, individual companies would have an incentive to adhere to the guidelines in order to attract customers.

Another major implementation challenge concerns the potential motivation of consumers to utilize KIPPs. One of the primary reasons why privacy notices are often disregarded today is because consumers are overburdened with the policies of a plethora of different companies, most of which are written in abstruse language. However, past research suggests that consumers would utilize privacy policy information more in their online decision-making if the saliency of important privacy information is increased (Tsai et al., 2011). KIPPs could help accomplish this goal by improving the comprehensibility of privacy notices. This would allow consumers to more easily interpret the important terms and conditions within notices, which might stimulate higher readership rates.

Network effects also detract consumer attention away from privacy notices. As more people use a particular social media website, the website becomes more valuable for its users. This creates a greater incentive for consumers to use the website, and a reduced incentive for consumers to read the website's privacy policy. KIPPs could potentially reduce these types of network effects by raising consumer awareness of the importance of privacy notices. If consumers read notices more frequently because they were able to better understand their contents, consumers would likely be more inclined to use websites with greater privacy protections.

Responses to the survey question displayed in Figure 1 above provide support for this idea. In the question, about 43% of respondents (n=707) indicated that they had previously decided not to use a website strictly because of the website's privacy policy (PP) or terms of service (ToS) agreement. By correlating these responses with two other questions concerning readership rates for privacy notices, we found that people who read PPs and ToS agreements more often were more likely to have refused to use a website strictly because of the website's privacy notice. These correlations were very strong (For PP readership, $r = .50$, $p < .01$) (For ToS readership, $r = .50$, $p < .01$), suggesting that the relevance of privacy notices would increase if people read them more frequently. Although the implementation of KIPPs alone would not likely cause all consumers to change their readership behavior, we expect that many consumers would read privacy notices more often if the notices were constructed around their preexisting knowledge.

Conclusion

Deficiencies in consumer knowledge must be addressed in order to improve the effectiveness of the existing "notice and choice" approach to digital privacy. Privacy notices could likely play a greater role in informing consumer decision making if they better accommodated the needs of diverse individuals with varying degrees of background knowledge. In this paper, we have proposed a new instrumentality, the Knowledge-based Individualized Privacy Plan (KIPP), which would aim to improve consumer comprehension of the significance of privacy notices by personalizing information based on different levels of preexisting knowledge. We are enthusiastic about the potential contributions that KIPPs could make as a tool to improve the effectiveness of notices within the "notice and choice" approach to digital privacy.

In order to be useful in an ever-changing online environment, KIPPs will need to address the needs of consumers, businesses, and relevant third parties. Thus, future research is needed to examine the practicality, usability, and design of KIPPs, as well as potential ways to increase consumer demand for more comprehensible privacy notices. In addition, more research is needed to assess what consumers from across the world currently understand about digital privacy and related issues. Performing this type of research will be crucial in order to guide future efforts, such as those related to KIPPs, aimed at increasing consumer privacy knowledge and promoting informed consumer decision-making.

References

Cranor, L.F. “Necessary but not sufficient: Standardized mechanisms for privacy notice and choice”, *Journal of Telecommunications and High Technology Law*, 10(2), 2012.

McDonald, A. M., & Cranor, L. F. “The cost of reading privacy policies”, *Journal of Law & Policy Information Society*, *4*, pp. 543, 2008.

Nissenbaum, H. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

Solove, D. “A taxonomy of privacy”, *University of Pennsylvania Law Review, 154*(3), pp. 477-564, 2006.

Tsai, J. Y., Egelman, S., Cranor, L. F., Acquisti, A. “The effect of online privacy information on purchasing behavior: an experimental study,” *Information Systems Research, 22*(2), pp. 254-268, 2011.

United States Census: Educational Attainment [Online], 2009. Available: http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_09_1YR_S1501&prodType=table

U.S. Department of Education, "Individualized Education Program." *IDEA - Building The Legacy of IDEA 2004*. 4 Oct. 2006. Web. 02 May 2014.