Using Experiential Learning to Effectively Inform People About Web Privacy Risks

Emergent Research Forum (ERF)

Claus-Peter H. Ernst
Frankfurt University of Applied Sciences / SRH University Heidelberg
cernst@fb3.fra-uas.de / claus-peter.ernst@srh.de

Birte Malzahn
Hochschule für Technik und Wirtschaft Berlin
birte.malzahn@htw-berlin.de

Katharina Simbeck
Hochschule für Technik und Wirtschaft Berlin
katharina.simbeck@htw-berlin.de

Abstract

Using the web carries risks for people's privacy. In order to enable people to protect themselves, they need to know about the potential threats associated with surfing the web. Based on the theory of constructivism, we argue that people better assimilate knowledge regarding privacy risks on the web when they actively experience these risks, rather than passively learn about them. More specifically, we hypothesize that methods requiring high learner engagement are more effective at conveying web privacy risks than those that require low learner engagement. In order to empirically evaluate our hypothesis, we plan to conduct an experiment. More specifically, we seek to compare the privacy risk levels of three groups: a control group, a group that simply reads about the potential negative outcomes of being tracked, and a group that experiences their individual surfing behavior being tracked.

Keywords

Privacy Risk, Experiential Learning, Constructivism.

Introduction

The web has become ubiquitous in many aspects of people's daily lives. However, using the web and its services carries risks, especially in terms of people's privacy (cf. Ernst et al. 2015). In addition, many people are unfamiliar with the risks associated with surfing the web. Indeed, information technology can collect web users' personal data, i.e., any data that involves information about the specific web user including their behavior, and without them noticing. For this reason, users often lack a clear understanding of what aspects of their personal information other people or institutions can collect, how that information can be used, and what consequences this might have (Acquisti et al. 2015).

It has been shown that perceived risk, in general, is able to alter people's behavior with regards to technology and media (e.g., Featherman and Pavlou 2003; Jarvenpaa et al. 2000; Malhotra et al. 2004; Pavlou 2001; Pavlou 2003). More specifically, when people are familiar with the potential negative outcomes associated with certain behaviors (Chen 2013, p. 1222; Sitkin and Pablo 1992), people do adapt their behavior in order to prevent these negative effects (e.g., Ernst et al. 2015).

The following question then arises: How can we effectively inform people about the potential privacy risks associated with their web usage behavior in order to enable them to better protect themselves? In this study, we draw from the theory of constructivism to propose a hypothesis regarding the effective conveying of web privacy risks. More specifically, the theory of constructivism postulates that knowledge has to be constructed by the mental activity of the learners themselves and cannot be successfully transmitted simply by passively receiving information (Driver et al. 1994). Based on this, we hypothesize that methods that require high learner engagement such as learning-by-doing are more effective at conveying web privacy risks than those that require low learner engagement such as reading textbooks.

In order to empirically evaluate our hypothesis, we plan to use one popular constructivism-based teaching method, i.e., experiential learning, which can also be described as learning from experience (Lewis and Williams 1994). More specifically, we plan to compare the Perceived Privacy Risk levels of three different groups (measured via a seven-point Likert-type scale consisting of three items identified in the literature): a control group, a group that experiences their individual surfing behavior being tracked, and a group that simply reads about the potential negative outcomes of being tracked.

The paper is organized as follows: In the next section, we will provide the theoretical background of Perceived Privacy Risk and introduce the theory of constructivism. Following this, we will present our research model and our planned research design.

Theoretical Background

Perceived Privacy Risk

People regularly provide their personal information on the web. In some cases, they do so willingly, such as in social network sites. In other cases, they might disclose personal information unwillingly or even unwittingly. For example, cookies – little pieces of information stored by websites on the computers of web users – enable websites to recognize and track computers. When visiting Amazon.com, the website places a cookie on your computer. When you visit the website again, it looks for a potential placed cookie, finds it, and knows, based on the information of the cookie, that you are you, and, for example, is able to provide personalized product suggestions. In addition to first-party cookies that originate directly from websites a web user knowingly accessed, cookies can also be placed by third-parties, i.e., companies that are *connected* to the website actually visited. As a result, within a short time frame, normal web browsing leads to the storage of numerous different cookies on users' computers, enabling visited websites as well as additional third parties to track users' behavior across the web. In consequence, regular web surfing behavior can carry risks in terms of people's privacy.

Privacy is "the claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1968, p. 7). Risk can be generally described as "the extent to which there is an uncertainty in significant and disappointing outcomes that may be realized" (Chen 2013, p. 1222; Sitkin and Pablo 1992) and Perceived Risk is consistently understood as "the expectation of losses associated with … [specific actions]" (Peter and Ryan 1976, p. 185). Drawing from these definitions, we define Perceived Privacy Risk in our context as the degree to which a person believes that surfing the web has negative consequences with regards to their privacy.

It has been shown that different kinds of Perceived Risk can exert an influence on people's behavior (e.g., Tan 1999). This influence has been a popular topic in previous research, especially in studies related to e-commerce and e-services. Indeed, multiple studies confirmed the existence of a negative influence of Perceived Risk on the usage of such services and their associated products (e.g., Featherman and Pavlou 2003; Jarvenpaa et al. 2000; Malhotra et al. 2004; Pavlou 2001; Pavlou 2003).

Constructivism

According to the theory of constructivism, people's knowledge evolves through interactions with the environment (Savery and Duffy 1995). More specifically, constructivism postulates that knowledge cannot be successfully transmitted in traditional teacher-centered teaching where learners only passively receive information from their instructor. Rather, knowledge has to be constructed by the mental activity of the learners themselves (Driver et al. 1994) while "… doing things and thinking about the things they are doing" (Bonwell and Eison 1991, p. 19). In other words, learners actively construct meaningful knowledge from their individual experiences based on their active participation in solving real and authentic problems and in critical thinking (Kridel 2010; Michael 2006).

The efficacy of constructivism-based (inter)active learning strategies has been confirmed several times. For example, Öhrn et al. (1997) found that students that used interactive computer programs to study had significantly better test results than students that learned via a traditional textbook. Hake (1998) showed that the use of interactive methods improved the conceptual understanding and problem-solving abilities of students enrolled in introductory physics courses. McCarty and Anderson (2000) compared active learning techniques with traditional teaching styles and found that active learning lead to more successful

learning outcomes in the case of history and political science students. Freeman et al. (2014) showed that the performance of science, technology, engineering, and mathematics students increased by applying active learning techniques. See Michael (2006) for an extensive collection of studies that underline the efficacy of constructivism-based learning strategies.

Research Model

Surfing the web carries risks with regards to people's privacy (e.g., Ernst et al. 2015), since people cannot know and/or control how, when, or to what extent, someone might (mis)use their personal information (cf. Westin 1968). It has been shown that Perceived Risks can exert an influence on people's behavior (e.g., Tan 1999), such as altering one's behavior in order to protect oneself from the potential negative effects of these (perceived) risks (e.g., Ernst et al. 2015). However, objective privacy risks and the perception of privacy risk are not necessarily fully congruent. Indeed, if a web user does not know anything about the privacy risks on the web and the potential negative outcomes of these risks, their perception of privacy risks may be low, although objectively these risks would be high. People thus need to be effectively informed about the potential privacy risks on the web, in order to enable them to protect themselves.

Based on the theory of constructivism, we believe that knowledge regarding privacy risks on the web cannot be most effectively conveyed by only providing this information in textual form (Driver et al. 1994). Rather, people need to actively construct this knowledge from experiences they actively participate in (cf. Kridel 2010; Michael 2006). We hypothesize that: *Methods that require high learner engagement are more effective in conveying the privacy risks associated with web use than methods that require low learner engagement.*

Outlook

We plan to use one popular constructivism-based teaching method, i.e., experiential learning (Lewis and Williams 1994) in order to empirically evaluate our hypothesis. More specifically, we plan to compare the Perceived Privacy Risk levels of three groups: a control group that will receive no information pertaining to web-tracking privacy risks, a group that experiences their individual surfing behavior being tracked, and a group that simply reads about the potential negative outcomes of being tracked. The following paragraphs describe our approach.

One popular constructivism-based teaching method is experiential learning, which can also be described as learning by doing or learning from experience (Lewis and Williams 1994). "Experiential education first immerses […] learners in an experience and then encourages reflection about the experience to develop new skills, new attitudes, or new ways of thinking" (Lewis and Williams 1994, p. 5).

In order to evaluate our hypotheses, we plan to use an experiential learning situation involving the Firefox web browser and its add-on Lightbeam. "When you activate Lightbeam and visit a website, sometimes called the first party, the add-on creates a real-time visualization of all the third parties that are active on that page … As you then browse to a second site, the add-on highlights the third parties that are also active there and shows which third parties have seen you at both sites. The visualization grows with every site you visit and every request made from your browser" (Mozilla Foundation 2016). For example, Figure 1 presents an adjusted screenshot of Lightbeam's visualization after visiting the websites of The New York Times and CNN. The graph shows that both sites (represented as circles) establish connections with numerous third-party servers (triangles and lines). Some of these third-party servers set cookies on the user's computer (purple lines). The third-parties in the middle of the graph, such as Facebook, record the visit to both sites and are thus able to recreate the user's browsing interests in this case.

More specifically, we plan to survey students from a German university attending a Business Administration lecture. In this manner, we plan to obtain at least 100 complete German-language questionnaires for each group. All respondents will have to answer a questionnaire consisting of three Perceived Privacy Risk items, which were identified in the literature and which will be measured using a seven-point Likert-type scale ranging from "strongly disagree" to "strongly agree" (see Table 1). Moreover, the questionnaire will include multiple controls for attributes that might play a role in the individuals'

choice of privacy-related behaviors, such as having been a victim of identity theft in the past, or having been scammed or misled on the web in the past.

Whereas the control group will only have to answer the questionnaire, the first treatment group will have to read an informational text about web tracking (see Table 2) before answering the questionnaire. The second treatment group will have to (i) use Firefox with the Lightbeam add-on activated and surf the web for 10 minutes on websites of their choice, (ii) look at the resulting visualization of Lightbeam, (iii) read the informational text about web tracking along with a Lightbeam interpretation aid (see Table 2), and then (iv) answer the questionnaire we created.

If our hypothesis is correct, the Perceived Privacy Risk levels of both treatment groups should be significantly higher than the levels of the control group. In addition, the Perceived Privacy Risk levels should be higher after surfing with Lightbeam than after simply reading the informational text.

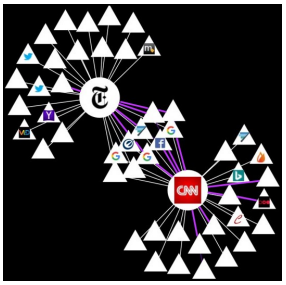

Figure 1. Adapted Lightbeam Screenshot

For this article, we made the purple lines slightly thicker than they were in the original screenshot, in order to make them more apparent in printing.

Construct	Items	Adapted from
Perceived Privacy Risk	If I do not protect my personal data on the web from tracking, others might misuse my personal data.	Chen (2013) Featherman and Pavlou (2003) Krasnova et al. (2010) (cf. Dinev and Hart 2006; Malhotra et al. 2004)
	If I do not protect my personal data on the web from tracking, I might lose control of the privacy of my personal data.	
	There is a threat to my privacy if I do not protect my personal data on the web from tracking.	

Table 1. Items of our Measurement Model

Informational text	Companies track your online activities, collect this data and use it in various ways. Have you ever experienced visiting a website, and afterwards, seeing advertisements for this company on other websites? This is what tracking is responsible for. Tracking enables companies to create profiles about users' behaviors and interests, which are also regularly resold to other companies. Tracking is used on all kinds of websites and can be done on your desktop computer, your laptop, and other mobile devices such as smartphones and tablets.
Lightbeam interpretation help	In the net-like graph, you can see the websites you have visited (represented as circles), as well as the calls triggered to third-party servers (represented as triangles). If multiple websites trigger calls to the same third-party servers, these servers record your visit to all corresponding websites and are, hence, able to track your corresponding online activities.

Table 2. Informational Text and Lightbeam Interpretation Aid

If confirmed, our study will contribute to the literature on privacy and pedagogy by emphasizing that in order to effectively convey privacy risks, people need to be engaged in the learning process, such as in experiential learning situations. Our results would also hold important practical implications. More specifically, if confirmed, our findings would suggest that simply informing people about potential risks on the web through informational texts is insufficient. Rather, greater learning success would be achieved using methods that require high learner engagement, that is, that enable people to experience these risks with their own personal data and surfing behaviors. This insight would be especially important for teachers, instructors and lecturers in the context of schools and even universities.

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509-514.

Bonwell, C. C., and Eison, J. A. 1991. "Active Learning: Creating Excitement in the Classroom." The George Washington University: ASHE-ERIC Higher Education Report No. 1.

Chen, R. 2013. "Member Use of Social Networking Sites - an Empirical Examination," *Decision Support Systems* (54:3), pp. 1219-1227.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Driver, R., Asoko, H., Leach, J., Mortimer, E., and Scott, P. 1994. "Constructing Scientific Knowledge in the Classroom," *Educational Researcher* (23:7), pp. 5-12.

Ernst, C.-P. H., Pfeiffer, J., and Rothlauf, F. 2015. "Privacy Protecting Behavior in Social Network Sites," in *Factors Driving Social Network Site Usage,* C.-P. H. Ernst (ed.), Wiesbaden: Springer Gabler, pp. 57-81.

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.

Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., and Wenderoth, M. P. 2014. "Active Learning Increases Student Performance in Science, Engineering, and Mathematics," *Proceedings of the National Academy of Sciences of the United States of America* (111:23), pp. 8410–8415.

Hake, R. R. 1998. "Interactive-Engagement Versus Traditional Methods: A Six-Thousand-Student Survey of Mechanics Test Data for Introductory Physics Courses," *American Journal of Physics* (66:1), pp. 64-74.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. 2000. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:1/2), pp. 45-71.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Kridel, C. 2010. *Encyclopedia of Curriculum Studies*, Thousand Oaks, CA: Sage.

Lewis, L. H., and Williams, C. J. 1994. "Experiential Learning: Past and Present," *New Directions for Adult and Continuing Education*:62), pp. 5-16.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

McCarty, J. P., and Anderson, L. 2000. "Active Learning Techniques Versus Traditional Teaching Styles: Two Experiments from History and Political Science," *Innovative Higher Education* (24:4), pp. 279-294.

Michael, J. 2006. "Where's the Evidence That Active Learning Works?," *Advances in Physiology Education* (30:4), pp. 159-167.

Mozilla Foundation. 2016. "Lightbeam for Firefox 1.3.1." Retrieved 01-16, 2018, from http://addons.mozilla.org/de/firefox/addon/lightbeam.

Öhrn, M. A. K., van Oostrom, J. H., and van Meurs, W. L. 1997. "A Comparison of Traditional Textbook and Interactive Computer Learning of Neuromuscular Block," *Anesthesia & Analgesia* (84:3), pp. 657-661.

Pavlou, P. A. 2001. "Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation," *AMCIS 2001 Proceedings*, Paper 159.

Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 69-103.

Peter, J. P., and Ryan, M. J. 1976. "An Investigation of Perceived Risk at the Brand Level," *Journal of Marketing Research* (13:2), pp. 184-188.

Savery, J. R., and Duffy, T. M. 1995. "Problem Based Learning: An Instructional Model and Its Constructivist Framework," *Educational Technology* (35:5), pp. 31-38.

Sitkin, S. B., and Pablo, A. L. 1992. "Reconceptualizing the Determinants of Risk Behavior," *The Academy of Management Review* (17:1), pp. 9-38.

Tan, S. J. 1999. "Strategies for Reducing Consumers' Risk Aversion in Internet Shopping," *Journal of Consumer Marketing* (16:2), pp. 163-180.

Westin, A. F. 1968. *Privacy and Freedom*, New York, NY: Atheneum.