A Heuristic Evaluation of the Facebook's Advertising Tool Beacon

Arshad Jamal
Dept of Information Systems & Computing
Brunel University, West London, UK
Arshad.jamal@Brunel.ac.uk

Melissa Cole
Dept of Information Systems & Computing
Brunel University ,West London, UK
Melissa.cole@Brunel.ac.uk

***Abstract*—Interface usability is critical to the successful adoption of information systems. The aim of this study is to evaluate interface of Facebook's advertising tool Beacon by using privacy heuristics [4]. Beacon represents an interesting case study because of the negative media and user backlash it received. The findings of heuristic evaluation suggest violation of privacy heuristics [4]. Here, analysis identified concerns about user choice and consent, integrity and security of data, and awareness and notice. Beacon was an innovative tool, therefore, its systematic evaluation was needed in order to identify privacy problems, their causes and subsequent consequences. The study provides useful insights to human computer interaction (HCI) designers of online social networks.**

Keywords— Usability; privacy; security; heuristic evaluation; non-functional requirements (NFRs); social networking site (SNS); human computer interaction (HCI); control

I. INTRODUCTION

One of the most popular and largest social networking site (SNS), Facebook [1] which has over 200 million users and which ranked number 4 in the top 10 websites [2] , launched a new marketing tool called Beacon on the 6th November 2007. The purpose of Beacon was to provide an alternative approach to personalized marketing. The main idea was to use social networks by online businesses such as eBay and Fandango to allow users to send stories of their actions performed on websites of these businesses to their friends via automatic news feed. The actions could be for example, posting of an item for sale or renting a movie. When a user performed such an action on participating business website, a Beacon alert (figure 1&2) prompted user to send this 'story' to Facebook friends unless user opt-out of this action. Beacon alert which indeed was elusive since there was no prior notice given to user about what is Beacon and what it is going to do. Soon after it's launch, Beacon received negative press and user backlash. Consequently, Facebook had to withdraw Beacon, one month after the launch.

Undoubtedly, Beacon was an innovative tool which was withdrawn due to privacy concerns. Therefore, it's systematic privacy evaluation is required to identify the causes and consequences of privacy problems experienced by users of SNS.

Heuristics evaluation [3] is a well known method which is used to find usability problems in a user interface. Small number of evaluators usually 3-5 [3] [4] examine interface to check compliance of principles called 'heuristics'. It is an informal and cheap method which can be used by novices, usability experts or double experts who have usability as well as application domain knowledge [3] [4]. 3-5 double experts can find between 81% and 90% problems, regular experts can find between 74% and 87% problems and five novices can find 51% of problems [4].

The aim of this research therefore, is to evaluate the usability problems in Beacon experienced by Facebook users regarding their privacy management. This will be achieved specifically by conducting a heuristic evaluation on the marketing tool Beacon using privacy heuristics [7] [8]. These findings are then discussed and insights offered for HCI designers of social networks.

II. PRIVACY AND PRIVACY FRAMEWORKS

A. What is Privacy?

The concept of privacy includes issues such as personal information control, personal autonomy, individual secrecy and protected access to places and bodies [9]. Although the collection of information by organizations is important for customer service, [10] argues that the "indiscriminate collection and retention of data represents an extraordinary intrusion on privacy of individuals". But what does 'indiscriminate' mean in an online network characterized by the sharing of social and private information?

One way of addressing this question is to view privacy as an HCI problem. Privacy frameworks relevant to HCI researchers and practitioners can be roughly grouped into two categories:

(i) Guidelines, such as Fair Information Practices [11]. This was an early design guideline aimed at supporting data protection legislation and offers a system-centred view.

(ii) Process Frameworks such as STRAP [7][8] or Questions Options Criteria (QOC) process [12]. These provide guidance on the analysis and design of privacy-sensitive IT applications and have a user-centred focus.

B. Privacy Framework: Structured Analysis of Privacy

Structured Analysis of Privacy (STRAP) framework [7] [8] offers 11 dedicated set of privacy heuristics intended for use by designers to analyze interactive systems. See table 1 for details of heuristics. Modelled on usability heuristics [3] and fair information practices [11], the STRAP framework is a structured means of analyzing non-functional user requirements (NFRs) [7] [8]. There are two reasons to choose STRAP heuristics for the evaluation of Beacon. First is the assumption that designers are generally not good at addressing a social issue (e.g. privacy) in the design of information systems. Thus, they need an easy to use and light weight (easy to learn) tool to address social issues like privacy. Secondly, because of the benefits associated with heuristic evaluation method and it's reputation as a cheap and effective method [3] [4].

Moreover, STRAP heuristics were tested for efficiency and effectiveness by [8] and found the tool useful to discover privacy, security and associated usability problems. By efficiency [8] means e.g. how many privacy problems can be located in unit time and effectiveness means total number of privacy issues found as effectiveness. However, this study is the first that uses STRAP heuristics [7] [8] in the privacy evaluation of online social networks.

III. HEURISTIC EVALUATION OF BEACON

A. Evaluators and evaluation process

Three evaluators performed heuristic evaluation of Beacon using STRAP heuristics [7]. All three evaluators including author 1 have HCI background and experience of using heuristic evaluation method. They also have profiles on Facebook. Author 1 also has background domain knowledge of privacy theories and principles. Therefore, the team has expertise in both heuristic evaluation method and the domain knowledge. Each evaluator performed evaluation separately to avoid influence of one evaluator's work on the other. Each evaluator applied 11 privacy heuristics [7] on Beacon interface (shown in figure 1&2) to see whether it is violated or not. Three lists of evaluations are produced. Subsequently, each evaluator recorded severity rating of violated privacy heuristics. Each problem is measured along a continuous scale: very serious, serious, minor, and no problem. Following severity ratings are used as suggested by [6]: 0= I don't agree that this is a usability /privacy problem; 1= Minor problem and should not be given low priority; 2= Serious problem and should be given high priority, 3=Very serious problem and should be given very high priority. Three lists of individual severity ratings are compiled into a single list. The mean severity ratings and standard deviation (SD) of each problem are computed. We also computed complete consensus (as a percentage) to show consistency between the ratings.

B. Analysis of Results

Table 2 provides a breakdown of the usability problems encountered in Beacon and shows the means and standard deviations of severity ratings of the problems.

TABLE I. STRAP HEURISTICS [4][5]

Heuristic		Description
Notice /Awareness	***Available, Accessible and clear***	Make information about the systems activities always available to users and simple to access and understand
	Correct, Complete and consistent	Ensure that disclosures are complete, correct and consistent for users to make informed decisions
	Presented in context	Relevant information should be presented for each transaction to minimize memory load and ensure users are aware of consequences of actions
	Not overburdening	Disclosure must take into account human limitations in memory, ability and interest. Provide succinct and relevant information
Choice /Consent	***Meaningful Options***	Users need to be given real options rather than opt-in/opt-out when possible to avoid coercion and maximize benefits
	Appropriate defaults	Default settings should reflect most users' concerns and expectations about privacy
	Explicit consent	Avoid assuming consent whenever possible.
Integrity / Security	***Awareness of security mechanisms***	Users should be provided with enough information to judge security of system and their information
	Transparency of transactions	Systems should provide transparency of transactions and data use to build user confidence and trust
Enforce/ Redress	***Access to own record***	Users should have access to all information the system has collected about them, regardless of source
	Ability to revoke consent	Consent should be retractable

Figure 1. Early Beacon Alert

Figure 2. Final Version of Beacon Alert

TABLE II. HEURISTIC EVALUATION OF BEACON USING STRAP

Problems in Beacon	Mean Severity Ratings	Standard Deviation	Complete Consensus
Lack of availability, accessibility and clarity of system information to user.	2.67	0.58	67%
Notices to users are not correct, complete and consistent.	2	0	100%
Relevant background information to users is not given for each transaction to understand the context.	2	1	33%
Disclosure of information is not succinct and relevant rather user was not provided with complete information.	1.33	1.15	67%
Users are not given meaningful options to accept a service or feature or reject it.	3	0	100%
Default settings do not reflect most users' concerns and expectations about privacy, e.g. *beacon uses opt-out and users expected opt-in*.	3	0	100%
Explicit consent is not obtained.	2.33	0.58	67%
Users are not given enough information to judge security of system and their information.	3	0	100%
System does not provide transparency of transactions and data use to build user confidence and trust.	3	0	100%
Users do not have access to all information the system has collected about them, regardless of source	1.33	1.53	33%
Consent cannot be revoked	3	0	100%

The mean severity rating of 3 shows a very serious problem where as 0 shows the absence of problem. For an illustration, problem 6 has mean severity rating of 3, SD of 0 and complete consensus 100%. Because all three evaluators gave a rating of 3 to problem 6 which states that *'Default settings do not reflect most users' concerns and expectations about privacy e.g. beacon uses opt-out and users expected opt-in'*. Therefore, the mean severity rating for this problem is 3, with zero SD and 100% complete consensus. Out of 11 problems, 5 problems (46%) were very serious, 4 problems (36%) were serious, and 2 problems (18%) were minor problems. So, 82% of problems were serious. For all 5 very serious problems, SD is 0 and there is complete consensus (100%) among the raters. Such high percentage of problems discovered in Beacon improves our understanding of the causes of severe user backlash and subsequent withdrawal of Beacon by the Facebook.

The mean of the SD of all ratings is 0.44 which shows that severity ratings of evaluators are only dispersed marginally. To measure reliability and consistency of rater's ratings, we computed general measure of agreement between raters. For example, the general measure of agreement between rater 1 and rater 2 is 70%, between rater 1 and rater 3 is 60% and between rater 2 and rater 3 is 70%. The mean general measure of agreement between raters is 67% which is acceptable.

IV. DISCUSSION

It is clear from the privacy-focused heuristic evaluation of Beacon that all 11 heuristics were violated with the greatest violations occurring with three privacy issues: user choice and consent; notice and awareness; and integrity and security of data. The first two privacy issues are generally recognized by the HCI community to be the core principles for the successful design of software applications. The issue of notice and awareness is challenging for designers to determine a striking balance between notices for awareness and minimum distraction for the users. These two issues together determine the level of control users have when they perform any action that requires sharing of personal information. On this occasion users were not given control on the use of personal information. This finding is in line with study performed by [13] to measure internet users' information privacy concerns. According to [13], control is important to determine information privacy and can be exercised via approval, modification, and choice to opt-in or opt-out. Beacon clearly made basic design errors and consequently end user was completely ignored. For example, user was not given a universal opt-out of automatic feeds and had to opt-out on each occasion separately shows the bad intention to force user into accepting the automatic feeds by default. Surely, the user was not given control or freedom or authority to select or avoid sending user stories to a third party website.

The third privacy issue, integrity and security of data, appears to reflect the unique concerns of sharing personal information online. The negative press and user outrage expands this by highlighting a user's desire to be explicitly consulted by third parties who wish to use and transfer personal data. Users were not informed of the presence of Beacon and also about its purpose. Consequently, users were alarmed when their stories of actions on participating

business sites were published on their Facebook news feed.

Also, the users lost faith on third party organizations and their integrity was also questioned. End users were not sure that their individual interests would be protected when their personal browsing interests were automatically distributed across their 'friends' network. In this instance, users were primarily concerned with conducting a risk analysis on the indiscriminate transfer of personal information.

Viewing privacy as risk analysis in online social networks raises two set of interesting points for HCI designers to consider. According to [14] the first set of points (a, b, c, d) relate to the social and organizational context whilst the second set (i, ii, iii) highlight the nature and purpose of the technology used. With regard to user perceptions of Beacon, key questions to ask could include:

a) Who are the people sharing personal information (data sharers) and who are the people that see the personal information (data observers)?

b) What kinds of personal information are shared and under what circumstances?

c) What is the value proposition for sharing information?

d) Are their third parties that might be directly or indirectly impacted?

i) How is personal information collected and shared? (Opt-in / opt-out; pull / push)

ii) How much information is shared? Is it discrete or continuous?

iii) What is the quality of the information shared and how long is personal data retained?

V. CONCLUSION

Beacon was a novel marketing tool within the massively growing online social network environment. Beacon damaged the reputation of Facebook as well as third party organizations and consequently withdrawn due to lack of understanding of the nature of privacy in social network. Our findings of the case study of Beacon confirms the arguments of [15] that privacy should be viewed as a holistic feature of interactive systems and a poor interface or design component that leaks personal information and which is not usable may damage reputation of interactive systems [15].

Usability property of privacy brings three facts into light in social networks (i) consent and choice and (ii) notice and awareness (iii) third party integrity and security of transmitted data.

Designers of social networks need to be aware of the sensitivity of user information. Specifically, they need to have a better view of the interaction between the social and organizational context. They also need to adhere the socio-technical context of socially networked information (e.g. How is information shared and who has the control?). This study suggests that the individual users prefer to retain control over the type and nature of information shared. An interesting area for future research would be to determine the form and extent of user control using the risk analysis questions presented above. Finally, we have seen that media has played an important part to not only bring awareness among users regarding the risks associated with their information , but also has motivated them to raise their voice and force providers to redesign privacy invasive features. Therefore, an interesting area of future research would be to investigate user behaviour to privacy breaches in social networks especially through a longitudinal study.

REFERENCES

1. Facebook's advertising tool Beacon information can be found at: http://www.facebook.com/business/?beacon accessed May 2008.
2. Top global websites. http://alexa.com/topsites , viewed May 10, 2009.
3. Nielsen, J. and Molich, R. (1990), "Heuristic evaluation of user interfaces", Proc. ACM CHI'90 (Seattle, WA, 1–5 April 1990), 249–256.
4. Nielsen, J.(1992),"Finding Usability problem through Heuristic Evaluation", Proc. ACM CHI '92.
5. Nielsen, J. (1994),"Heuristic Evaluation", In Nielson,J, and Mark, R.L.(1994.),Usability Inspection methods, John Wiley&Sons,New York,NY.
6. Nielson, J and Mack, R. L. (1994), "*Usability Inspection Methods",* John Wiley & Sons, Inc.
7. Jensen, C. (2004), "Toward a method for privacy vulnerability Analysis", CHI 2004, extended abstracts on Human factors in computing systems, Publisher: ACM
8. Jensen, Carlos and Potts, C. (2007), "Experimental evaluation of a lightweight method for augmenting requirements analysis" WEASELTech '07: Proceeding of the 1st ACM international workshop on Empirical assessment of software engineering languages and technologies: held in conjunction with the 22nd IEEE/ACM International. Conference on Automated Software Engineering (ASE) 2007
9. Kemp, R. and Moore, A., D. (2006), "Privacy", Library High Tech Vol. 25, No.1, 2007, pp 58-78 Emerald Group Publishing Limited.
10. Sushil, J.(1996), ,"Managing security and Privacy of Information", ACM Computing Surveys (CSUR), Volume 28 issue 4.
11. Organization for Economic Co-operation and Development (1980), "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Technical Report.
12. Bellotti, V. and Sellen, A. (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.
13. Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research (15:4), 2004, pp. 336-355.
14. Hong, J., Ng, J. D. , Lederer, S. and Landay, J. A. (2004), "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in Proceedings of Designing Interactive Systems (DIS2004), pp. 91-100. ACM Press, Boston, MA, 2004.
15. Iachello ,G. and Hong, J. (2007) "End user Privacy in Human Computer Interaction" Foundations and trends in Human-Computer Interaction Vol 1 ,No 1 , pp1-137