Privacy Preservation in Web Browsers through Privacy Enhancing Tools

Swarnangini Ghosh
Department of Computer Science and Engineering
Sagar Institute of Research & Technology,
Bhopal,India

Rajesh Shukla
Department of Computer Science and Engineering
Sagar Institute of Research & Technology
Bhopal, India

ABSTRACT
The Internet has revolutionized the way the world and everything around works. People today find it hard to imagine a world without electronic-mails and search engines where every piece of information is just a few clicks away. The use of social media, online banking services, emails and so on allow for many differernt details concerning our personal life to be stored and used online. Similarly misuse of our data by some unknown organisations is also not in our control. While accessible information about us is growing on the Internet, the potential ways to misuse or exploit them is likewise increasing. This has created privacy concerns and a need for better privacy control for users. It can be concluded from the literature survey, that more research in this area is restricted to conceptualization of privacy than a technological solution. The browsers act as an interface between the users and the Internet, hence more features need to be incorporated into them that can empower the users when interacting with the Internet. This paper emphasizes on the need for designing more privacy enhancing tools using a novel approach called Value Sensitive Design (VSD) which provides methods for creating and assessing a design outcome by taking human ethics into consideration.

General Terms
Privacy, Internet, Browser

Keywords
Information Privacy, Value Sensitive Design, Privacy Enhancing Tools (PETs), Privacy Concern, Internet Age.

1. INTRODUCTION
The Internet has evolved into a means of communication in a daily life; exchanging information, financial transactions, education, research, shopping, entertainment, social networking etc. It is a large market for companies that take the benefit of advertisements available at a low price and trade through the Internet, popularly known as e-commerce. It is a speedy way of communication for disseminating information to a large population at the same time.

Due to the remarkable growth of Information Technology, organizations are now more capable of accumulating and channelizing consumers' personal data. Privacy is therefore at the core of discussion as it affects several stakeholders that include IT professionals, business leaders, privacy advocates, government controllers and a common man. Day by day, an issue of privacy is becoming a matter of severe apprehension attributable to remarkable growth in technology. Invading user's privacy domain, using his personal information without taking his consent for commercial purposes, pose threat to his privacy that needs to be handled promptly with great severity.

The term Internet Privacy involves the right to privacy concerning storing, reusing, leaking and displaying of the information pertaining to an individual via the Internet. This is an important issue and challenge, attributable to all the information left and shared on the Internet and becomes a straightforward way to collect information about anyone without taking his consent. The Internet is international and largely unregulated [3], that means users from all over the world are at risk for privacy violations.

1.1. Internet Age
The Internet age is a period in an information era where communication and commerce became a central focus for customers, management, and the media. It also marks the convergence of the computer and telecommunication industries and their allied services and products. The Internet has revolutionized the way the world and everything around works. People today find it hard to imagine a world without electronic-mails and search engines where every piece of information is simple to find. The constant spread of information technology has several pervasive effects. An Internet age has a lot to offer and the opportunities are endless but with this it brings the possibility of this sparingly technology being the biggest threat to the safety of civilization. In current decades, there has been a constant development in the use and handling of vast quantities of personal data supported by computing technology. Though advancement in technology is essential to the progress of the world today, it has also opened up new avenues to misuse and exploit this information that people may regard as private data about themselves.

1.2. Informational Privacy
The term privacy is a large and somewhat distinct concept, with many definitions. Majority of people would still agree that it concerns the ownership of personal information and the owner's right to decide over it. The perception of privacy refers to the safety of the individual's distinctiveness or honor, as well as safeguarding his right to control the utilization and distribution of private information in relation to him. Hence privacy is an individual's legal right to decide over his own personal information [5].

The privacy of a consumer's personal information has become a significant public concern and is receiving increased attention from governments, legislative bodies and privacy promoters. According to the earlier researches, information privacy may be viewed as some rights, namely the right of individuals to choose what information about them to distribute to others, the right of individuals to be acquainted with information about them being collected, and the right of

individuals to use data. These three rights engross an individual's control over his personal information. Privacy can also be defined as the right of people to be in command of the use of their personal data.

A more important concern on the Internet today is that much of the information harvesting on the web is not known to users and thus beyond their control. Information about users' purchasing habit, online browsing activity and online movement is assembled, examined, utilized, and distributed, often without taking their consent. A technology that tracks online activity has become more advanced and invasive.

1.3. Privacy as a Design

In order to protect consumers' online privacy, several efforts as legal plans and technical solutions are made. Authorized approaches include National privacy regulations, guidelines, acts, privacy credentials and other privacy management checks that deal with the user's online privacy anxiety. This paper aims at highlighting the importance of designing a privacy enhancing tool to tackle the problem of online privacy although different legal approaches are available in different countries. This initiative is in consonance with a current analysis of the privacy literature that emphasizes the need for greater research in the area of information privacy for developing practical solutions [2].

1.4. Objective of Study

This paper makes you aware of the current challenges posed by an issue of privacy and encourages development of technical solutions to empower the user. To realize this goal, a detailed analysis of privacy literature was conducted and a conceptual analysis of privacy in an Internet age was performed. The objectives are further subdivided as

- Analysis of users' understanding of web browsers.
- Analysis of existing PETs for web browsers.
- Identify the need for designing PETs using VSD approach.

2. LITERATURE REVIEW

There are various researches concerning online privacy. In a research by Krishnamurthy et al., they analyzed some popular websites and found that some sensitive user information is leaked to the third-party aggregators [8]. The study conducted by Aggarwal et al. focused on private browsing modes and highlighted differences between the goals and implementations of such techniques [1]. Leon et al. investigated usability of various tools designed to curb the problem of online advertisement and discussed experiences of the participants [9].

2.1. Online Privacy Implications

New technology has always challenged the way people considered privacy and therefore the concept of privacy. An Internet age brings surge of changes, both fundamental and subtle, to the field of privacy and thus changes to the sparingly concept of privacy. Privacy is the ability to confer social associations by managing right to use information about oneself. Recent advancements in the area of technology and privacy have formed an environment that is both unsafe and promoting.

A recent poll showed that 59% of adults have refused to give information to an organization or business as everybody thought it absolutely was not necessary or was too personal. Many people upload their pictures on the Web and reveal their personal information on social networking sites. The repercussion of privacy invasion can be numerous, starting from loss of money, identity theft, and social status to even loss of life in almost extreme cases. The probabilities are not bounded that makes protecting this information more important than ever.

Since the vast amount of information is available freely on the Internet, an urgent need to secure online privacy of people, in this era of technological advancement is felt. Many areas are still unexplored within the field of online privacy. In precise, the Internet has improved the lives of people and has had more positive impacts as contrast to negative. Online privacy is a field that continues to remain unsafe if not given appropriate attention. The Internet is to disseminate Information to the masses thus issues, as security and privacy have not been on design priority. But efforts are essential to study these problems and develop solutions before it is too late.

2.2. Privacy Concerns

Several studies have reported growing consumer privacy concerns. The study revealed that user's attitude for privacy is totally dependent on the level and importance of the online transaction they are doing. Recent separate bodies of evidences show that although online users may have concerns about privacy, the value and convenience of online services outweigh privacy concerns [13].

The paradox between consumers' online privacy concerns and increased engagements with online activities have been explained by the fact that individuals have to give up some privacy to interact with the online world. Moreover, user's lack of information about privacy threats makes it complex for him to make correct assessments about privacy. Consumers are pursuing privacy according to their needs. When their needs are fulfilled, an issue of privacy becomes less significant. Thus the importance of privacy protection during an online transaction varies from person to person.

Privacy concerns are situations that arise when individuals can no longer be in charge of their personal information when surfing the Internet. In the present literature, the main consumer informational privacy concerns that have been used over the years are as follows:

- Uninformed access to personal information.
- Collection and dissemination of consumer personal information for commercial use, without taking his consent.
- Taking into consideration the concern over online tracking and the behavioral advertisement.

The way information is gathered on the Internet may not always be sparingly obvious. Sometimes the user is required to provide information by filling out an online form and sometimes cookies are used to gather information about them automatically. This creates different concerns for the users, both that information can be misused and that their surfing and activities can be tracked.

2.3. Browser Privacy Features

The browser is an interface between the Internet and several online users. Making the browser more controlling by incorporating security and privacy control tools can be equated with empowering online users. These features should be such that are easily traceable and user friendly. Recent

enhancements in browser features cannot rule out the need for strong privacy law, but users need to be given more power to make them more authoritative regarding their own data.

Recently many renowned companies have incorporated many features in the browsers to curb the growing problem of privacy. Use of the Internet is increasing day by day and so is the competition amongst popular browser vendors to provide more and more features to the users. Thus to fulfill the growing demand of users for security and privacy, they are incorporating the best possible features possible. When designing these features a trace is given on their simplicity and user-friendliness.

The browsers can specify what they can provide to the users by making necessary changes to privacy settings. These settings now decide how much information about an individual can be released to the outside world through cookies. The level of these settings if kept too high, browsers prevent certain websites to open properly. On the contrary, if these settings are kept too low, browsers release important information to the outside world inadvertently.

In general, various privacy enabling features are implemented in modern browsers as inbuilt settings, or extensions which allow the user to set opt-out cookies to block the third and/or first party cookies, to block ads and also Tracking Protection List (TPL), and set Do Not Track (DNT) preferences. The above -mentioned methodologies don't require an explicit assurance from the websites which may ignore the user privacy preferences. The following Table enlists the type of privacy features that are present in the major web browsers.

Table 1. Web Browsers Privacy Features

	Firefox	**Internet Explorer**	**Chrome**
Private Browsing	Yes	Yes	Yes
Managing Cookies	Yes	Yes	Yes
Do not track Header (DNT)	Yes	Yes	No
Tracking Protection List (TPL)	No	Yes	No
Plug-in	Yes	?	Yes

2.4. Privacy Enhancing Tools for Web Browser

The renowned browser vendors are incorporating many security and privacy features in their browsers for enabling users to freely interact with these browsers when surfing the Internet. Some of these features are Extended Validation SSL certificates [14], security cues, phishing warnings and security toolbars. All these features are put into practice using encrypted links with the websites to manage user's private data.

A lot of researches are conducted to discover the efficacy of these web browsers for supporting privacy and security issues of consumers. J. sobey et al. [14] carried out a user study to communicate status information about different types of certificates. They concluded that these certificates were overlooked in Firefox browser. In another study carried out by T. Whalen and K. M. Inkpen [15] have revealed that though web browsers support various features in the form of visual feedback mechanisms for securing online transactions, users pay less attention to these security cues when interacting with the Web.

Net Trust is a system that is designed by embedding social context in web based trust decisions for web browsers [7]. With the help of this an individual can select his own trusted sources of information to authenticate the reliability of a particular site. Any site can be rated as trustworthy based on trusted sources of information gathered from the market which are generated by ratings agencies and combining them with their individual social network. But the major flaw of the system lies in the fact that it cannot be used interactively while surfing the net, because its design is based on the concept of the user's post browsing considerations.

All popular browsers have incorporated several privacy control features as privacy controls, cookie controls, and object controls. They have also added private browsing modes to their user interfaces that ensure sites visited when browsing in private mode should leave no trail on users' computers. Also users should hide their identity from the web sites they visited. Nevertheless a study conducted by Aggarwal et al. [1] to evaluate the effectiveness of these privacy control features, including numerous add-ons, drawn an inference that flaws and susceptibilities exist in terms of how these browsers and add-ons approach protecting privacy and came to a conclusion that browsers sometimes leak information even in private browsing mode.

Microsoft Internet Explorer 9 supports a new customizable privacy control feature called Tracking Protection List (TPL) [10]. According to the information published on the official website of Microsoft, Tracking Protection helps users stay in control of their privacy when they surf the Internet. When browsing the web, certain advertisements, some links, pictures are displayed on the website that users visit by some third-parties. Although these contents can provide some enhancing features to the visited websites, they are generally meant to potentially track users' behavior across multiple sites. Microsoft offers a new feature called Tracking Protection to it's browser which provides help to the users by allowing them to set a list of the third party organizations which are allowed to collect their information and also the list of the organizations which they want to prevent from collecting their personal information. By adding a list, users can block content from websites that may have threat to their privacy. When users add a Tracking Protection List (TPL), Internet Explorer prevents their information from being sent by limiting data requests to websites in the list. For each list that users add, the setting applies across all pages and websites they visit, not just the pages they get the lists from. And each time they begin a new browsing session, the blocking stays on until they decide to turn it off. TPLs can be useful privacy tools but they cannot provide absolute protection or online privacy. Web sites added in TPL collect information and are responsible for their privacy policies and compliance. Any reliance users place on TPLs is strictly at their own risk. Since users usually think their online activities such as web browsing, checking email, online shopping, online banking, etc. as primary tasks, ensuring privacy through TPLs are overly burdened by them [10].

3. VALUE SENSITIVE DESIGN

Value Sensitive Design (VSD) is an initiative to develop an IT artifact that takes into consideration human ethics pursued all

through the development process [6]. In 1999, a report on VSD workshop emphasized VSD as an approach that is mainly apprehensive at values that focus on prosperity of the people to protect their pride, integrity, safety and privileges. These values include faith, responsibility, and freedom from injustice, access, autonomy, privacy, and authority. VSD is an approach that encourages interdisciplinary research by bringing people from different platforms in one place. Some people have expertise in developing computer systems and interfaces for the problem specified when others can be better known for their mastery over understanding ethics of people who are influenced by the system. Hence, the concepts and processes of VSD must be used in synchronization with the other accessibility techniques. Eventually, VSD enforces that we should widen the scope for evaluating the quality of technological systems by taking into consideration human values that form the base for human-computer interaction [6].

VSD adopts a novel and systematic way that revolves around a threefold approach that starts with the analysis of the concept followed by development and actual realization [6]. The main aim of this methodology is rigorous analysis of the concept under consideration that highlight the potential growth and technological challenges; design process focusing on architecture, user interface, simplicity and user friendliness and pragmatic approach to find views of people about the relevance of the software with the actual concept. The entire development process of the technical artifact focuses on human values. Some of the noteworthy applications developed using VSD approach are personal mobile safety [4], safeguarding children's online safety [16], groupware system [11] and web browser design [12].

4. RESEARCH METHODOLOGY

We have chosen survey methodology to gather users' requirements. The questionnaires were given to 100 students and faculties of Career College, Bhopal, MANIT, Bhopal and St. Theresa's Girls School, Bhopal. While developing an IT artifact, it is always necessary to understand the problem faced by the users in the current scenario, for which the artifact is proposed to be developed. The target user group selected for the survey was in the range of 13-34 years age group. The users of this range of age group are found to be more dependent on the Internet for various browsing activities like online shopping, social networking, studies, gaming, etc. They come under the target group which is online for most of the time. Faculties, on the other hand need to use computers for academic work, the amount of Internet usage and work makes it a reasonable justification to why the user group is chosen.

5. ANALYSIS

A qualitative methodology was adopted to analyze the users' responses to the questionnaire. The motto of this survey was to find out the difficulties faced by the users while surfing the Internet. Why users were not able to implement the various controls available in the browsers while navigating the Web? Why a need is felt to develop a PET to enhance the functionality of web browsers to provide better privacy control to the users? We regarded protecting one's online privacy as a sensitive topic. Consequently, there may be social implications to responses users give. The questions asked were aimed at understanding of users about web browsers, privacy awareness during online transactions and their dependence on Internet. The data collected was analyzed graphically and suggested a high level of agreement.

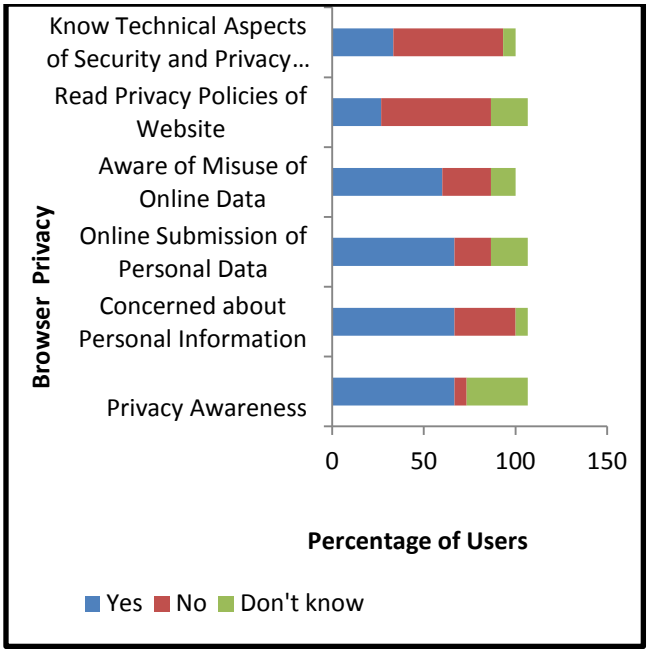

Fig. 1: User Awareness about Privacy

6. CONCLUSION

The review provides a comprehensive insight into the contemporary privacy concepts and emphasizes the need to protect privacy of consumers from a technological perspective. This analysis reveals that much of an individual's personal information can be collected, shared, exchanged, sold, and disseminated without consenting the individuals whose information pertains. Hence the individuals cannot protect themselves from online tracking as much of their behavioral information can be collected with the help of sophisticated mechanisms. This paper reviewed literature on privacy and found that research on informational privacy was more of theoretical than practical. A rigorous research is recommended to empower individuals when surfing the Internet. This can be achieved by providing them more control over their online data. Individuals interact with the web through browsers. Therefore, more privacy enhancing tools for web browsers need to be designed.

7. REFERENCES

[1] Aggarwal, G., Bursztein, E., Jackson, C., and Boneh, D. 2010. An analysis of private browsing modes in modern browsers. In Proceedings of 19th USENIX Conference on Security, USENIX Security'10, USENIX Association, Washington DC, pp. 1-15. http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf

[2] Bélanger, F., and Crossler, R.E. 2011. Privacy in the digital age: a review of information privacy research in information systems, MIS Quarterly vol. 35 (4), pp. 1-36. http://mdc.ltindia.com/librarym/mm_files/privacy%20in%20the%20digital%20age.pdf

[3] Chung, W., and Paytner, J. 2002. Privacy Issues on the Internet. In Proceedings of 35th Annual Hawaii International Conference on System Sciences, pp. 1-9. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.4421&rep=rep1&type=pdf

[4] Czeskis, A., Dermendjieva, I., Yapit, H., Borning, A., Friedman, B., Gill, B., and Kohno, T. 2010. Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety. In Proceedings of 6th SOUPS Symposium on Usable Privacy and Security, Redmond, WA USA, pp. 1–15. https://homes.cs.washington.edu/~borning/papers/czeskis-soups2010.pdf

[5] Datatilsynet, Privacy on 1-2-3 /What is privacy?[Online]. Available:http://www.datatilsynet.no/personvern/Hva-er-personvern/. Web-page retrieved on 22nd of June, 2013.

[6] Friedman, B., Kahn, P.H. Jr. and Borning, A. 2013. Value Sensitive Design and Information Systems, Early engagement and new technologies: Opening up the laboratory Philosophy of Engineering and Technology. vol. 6, pp. 55-95. http://www.e-reading.ws/bookreader.php/141465/Himma_-_The_Handbook_of_Information_and_Computer_Ethics.pdf

[7] Genkina, A., and Camp, L.J. 2005. Re-Embedding Existing Social Networks into Online Experiences to Aid in Trust Assessment, SSRN Working paper 707139. SSRN: http://ssrn.com/abstract=707139

[8] Krishnamurthy, B., Naryshkin, K., and Wills, C. 2011. Privacy leakage vs. Protection measures: the growing disconnect. In Proceedings of Workshop on Web 2.0 Security and Privacy. http://web.cs.wpi.edu/~cew/papers/w2sp11.pdf

[9] Leon, P. G., Ur, B., Balebako, R., Cranor, L. F., Shay, R., and Wang, Y. 2011. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In Proceedings 10th international conference on Privacy enhancing technologies, Carnegie Mellon CyLab, Technical Report. http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf

[10] Microsoft, Tracking Protection List, 2011. Available:http://ie.microsoft.com/testdrive/browser/TrackingProtectionLists/

[11] Miller, J.K., Friedman, B., and Jancke, G. 2007. Value Tensions in Design: The Value Sensitive Design, Development, and Appropriation of a Corporation's Groupware System. In Proceedings of International ACM Conference on Supporting Group Work, Sanibel Island, Florida, pp. 281-290. http://www.vsdesign.org/publications/pdf/miller_codecoop.pdf

[12] Millett, L.I., Friedman, B., and Felten, E. 2001. Cookies and Web Browser Design: Toward Realizing Informed Consent Online. In Proceedings of SIGCHI Conference on Human Factors in Computing Systems, ACM, Seattle, WA, pp. 46–52. http://www.cs.stevens.edu/~nicolosi/classes/sp08-cspriv/ref6-3.pdf

[13] Park, Y. J. 2011. Digital literacy and privacy behavior online, Communication Research. http://crx.sagepub.com/content/early/2011/08/19/0093650211418338.abstract

[14] Sobey, J., Biddle, R., Oorschot, P.C., and Patrick, A.S. 2008. Exploring User Reactions to New Browser Cues for Extended Validation Certificates. In Proceedings of 13th European Symposium on Research in Computer Security: Computer Security, Málaga, Spain, pp. 411–427. http://nparc.cisti-icist.nrc-cnrc.gc.ca/npsi/ctrl?action=rtdoc&an=8914096

[15] Whalen, T., and Inkpen, K.M. 2005. Gathering Evidence: Use of Visual Security Cues in Web Browsers. In Proceedings of Graphics Interface, Canadian Human-Computer Communications Society School of Computer Science Victoria, Ontario, Canada, pp. 137–144. http://pdf.aminer.org/000/236/079/gathering_evidence_use_of_visual_security_cues_in_web_browsers.pdf

[16] Xu, H., Irani, N., Zhu, S., and Xu, W. 2008. Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation. In Proc. 29th International Conference on Information Systems, Paris, pp. 1-9. http://www.cse.psu.edu/~szhu/papers/ICIS2008_COP.doc