



# TWO TALES OF PRIVACY IN ONLINE SOCIAL NETWORKS

Dr.M.V.Siva Prasad  
Principal & Professor

Anurag Engg College, Kodad, Nalgonda

Ch.Suresh Kumar  
Assistant Professor

Anurag Engg College, Kodad, Nalgonda

V.Ramya  
M. Tech Student, CSE

Anurag Engg College, Kodad, Nalgonda  
meetryamya@gmail.com

**Abstract**—Privacy is one among the friction points that emerges when communications get mediate in on-line Social Networks (OSNs). Totally different communities of technology researchers have framed the ‘OSN privacy problem’ in concert of police work, institutional or social privacy. In attempt these issues they have additionally treated them as if they were freelance. We argue that the different privacy issues square measure entangled which analysis on privacy in OSNs would get pleasure from an additional holistic approach. In this article, we tend to initial give associate introduction to the police work and social privacy views action the narratives that inform them, still as their assumptions, goals and ways. We then set the variations between these 2 approaches in order to know their complementarily, and to spot potential integration challenges still as analysis queries that so far are left unrequited.

**Key words:** OSN, UML, transparent, web server, issues

## 1. INTRODUCTION

Introduction Can users have reasonable expectations of privacy in Online Social Networks (OSNs) Media reports, regulators and researchers have replied to this question affirmatively, even in the “transparent” world created by the Face books, LinkedIn and Twitters of this world, users have legitimate privacy expectations that may be violate. Researchers from different sub-disciplines in computer science have tackled some of the problems that arise in OSNs, and proposed a diverse range of “privacy solutions”. These include software tools and design principles to address OSN privacy issues. Each of these solutions is developed with a specific type of user, use, and privacy problem in mind. This has had some positive effects: we now have a broad spectrum of approaches to tackle the complex privacy problems of OSNs. At the same time, it has led to a fragmented landscape of solutions that address seemingly unrelated problems. As a result, the vastness and diversity of the field remains mostly inaccessible to outsiders, and at times even to researchers within computer science who are specialized in a specific privacy problem. Hence, one of the objectives of this paper is to put these approaches to privacy in OSNs into perspective.

In the rest of this paper our goal is to show that even by looking at surveillance social privacy research, it can be argued that the time is ripe for a more holistic approach to privacy in OSNs. The article provides a comparative analysis of solutions addressing the surveillance and social privacy problems, and explores how the entanglement of these two types of problems can be addressed in computer science privacy research. We first look at the narratives that inform surveillance and social privacy problems in OSNs. We then provide an overview of the privacy solutions that aim to counter surveillance and, next, those that address social privacy problems in OSNs. Specifically, we focus on the underlying assumptions, problem definitions, methods and goals of the approaches. There are many subtleties that we brush over in order to accentuate the worldviews prevalent in the two approaches.

Privacy is one of the friction points that emerge when communications get mediated in Online Social Networks (OSNs). Different communities of computer science researchers have framed the ‘OSN privacy problem’ as one of surveillance, institutional or social privacy. In tackling these problems they have also treated them as if they were independent. We argue that the different privacy problems are entangled and that research on privacy in OSNs would benefit from a more holistic approach. In this article, we first provide an introduction to the surveillance and social privacy perspectives emphasizing the narratives that inform them, as well as their assumptions, goals and methods. We then juxtapose the differences between these two approaches in order to understand their complementarities and to identify potential integration challenges as well as research questions that so far have been left unanswered.

In the final section, we juxtapose their differences in order to understand their complementarities and identify research questions that so far have been left unanswered. By doing so, we not only put the different approaches into perspective, but we also start inquiring into a more holistic approach to addressing users’ privacy problems in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs.

## 2. PROPOSED SYSTEM

We distinguish three types of privacy problems that researchers in computer science tackle. The first approach addresses the “surveillance problem” that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers. The second approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short called “social privacy”. The third approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as “institutional privacy”.

typically tends to be large and extremely complex. It is crucial in such systems that the software is designed with a sound architecture. A good architecture not only simplifies construction of the initial system, but also, readily accommodates changes forced by a steady stream of new requirements.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects. Using the UML helps project teams communicate, explore potential designs, and validate the architectural design of the software.

The primary goals in the design of the UML are: Provide users with a ready-to-use, expressive visual modeling language so they can develop and exchange meaningful models. Provide extensibility and specialization mechanisms to extend the core concepts. Be independent of particular programming languages and development processes. Provide a formal basis for understanding the modeling language. Encourage the growth of the OO tools market. Support higher-level development concepts such as collaborations, frameworks, patterns and components. Integrate best practices.

## 4. IMPLEMENTATION & RESULTS

The most crucial phase of any project is the implementation. This includes all those activities that take place to convert from the old system to the new system. It involves setting up of the system for use by the concerned end user. A successful implementation involves a high level of interaction between the analyst, programmers and the end user. The most common method of implementation is the phased approach, which involves installation of the system concurrently with the existing system. This has its advantage in that the normal activity carried out, as part of the existing system is anyway hampered. The end users are provided with sufficient documentation and adequate training in the form of demonstration/presentation in order to familiarize with the system.

The way in which personal control and institutional transparency requirements, as defined through legislation, are implemented has an impact on both surveillance and social privacy problems, and vice versa. Institutional privacy studies ways of improving organizational data management practices for compliance, e.g., by developing mechanisms for information flow control and accountability in the back end. The challenges identified in this paper with integrating surveillance and social privacy are also likely to occur in relation to institutional privacy, given fundamental differences in assumptions and research methods.

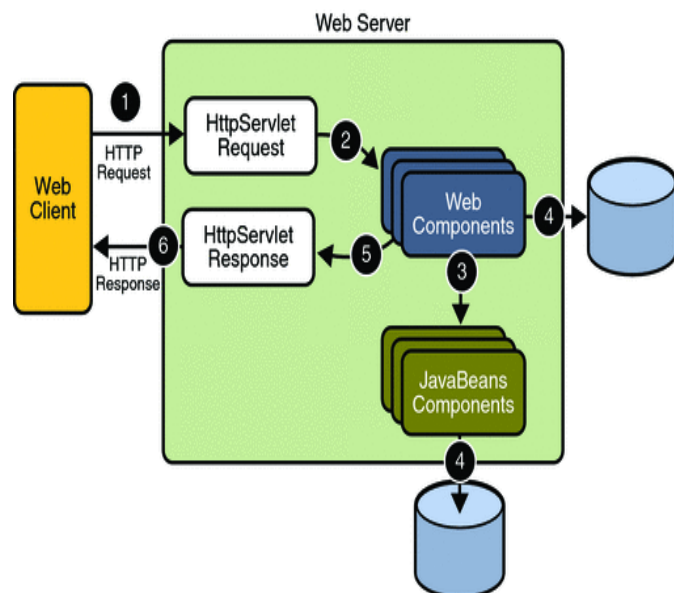


Fig:1. Content diagram of Project

## 3. DESIGN

Design is a meaningful engineering representation of something that is to be built. Software design is a process through which the requirements are translated into a representation of the software. Design is the place where quality is fostered in software engineering. Design is the perfect way to accurately translate a customer’s requirement in to a finished software product. Design creates a representation or model, provides detail about software data structure, architecture, interfaces and components that are necessary to implement a system. This chapter discusses about the design part of the project. Here in this document the various UML diagrams that are used for the implementation of the project are discussed.

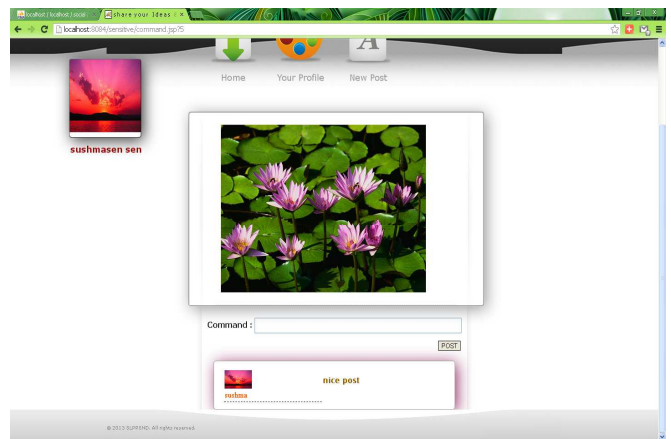
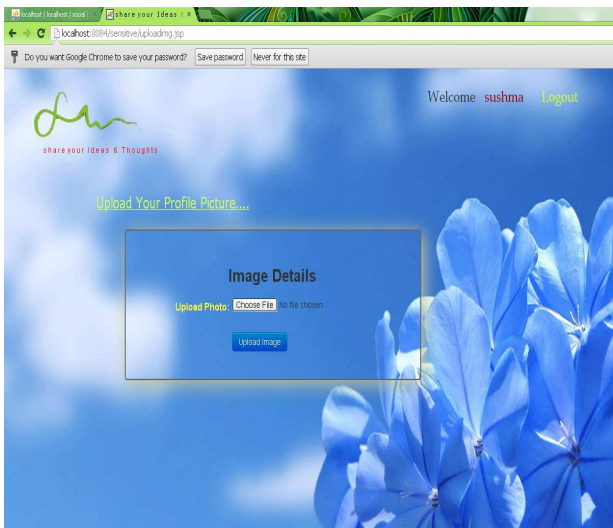
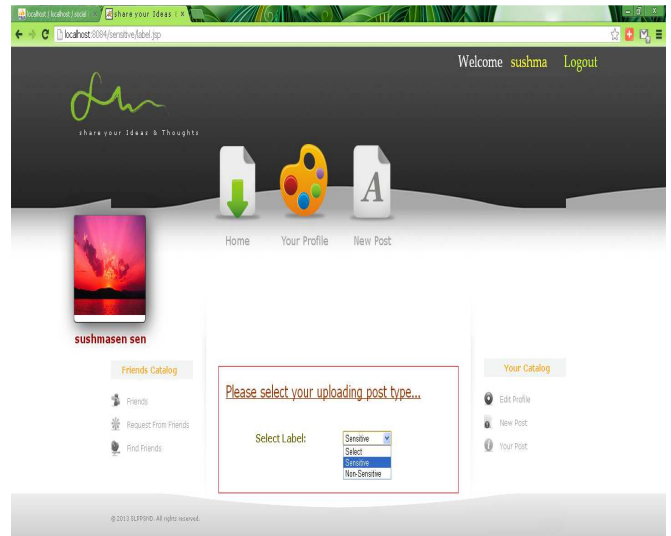
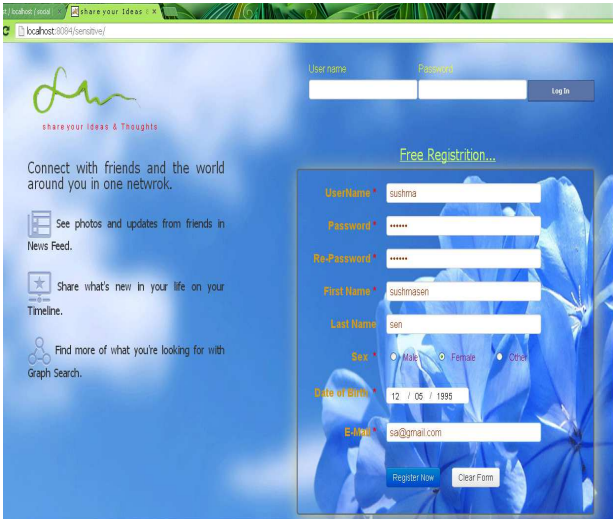
The Unified Modeling Language (UML) is a visual modeling language used to specify, visualize, construct and document a software intensive system. The embedded real-time software systems encountered in applications such as telecommunications, school systems, aerospace, and defense



# International Journal of Ethics in Engineering & Management Education

Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

## Output Screens

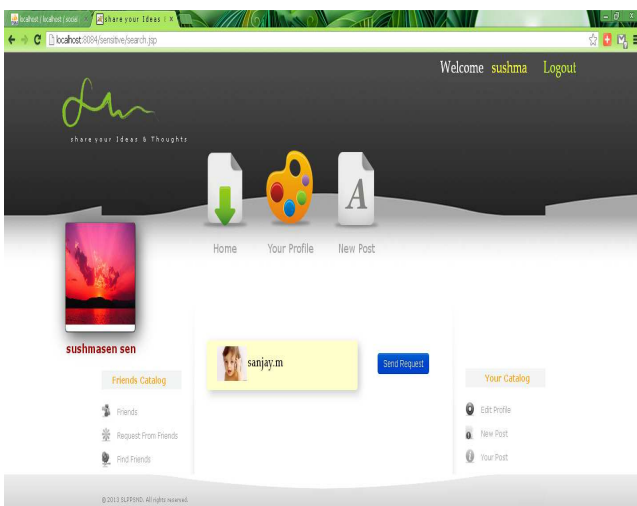


## 5. CONCLUSION

By just apposing their differences, we were able to identify how the surveillance and social privacy researchers ask complementary questions. We also made some first attempts at identifying questions we may want to ask in a world where the entanglement of the two privacy problems is the point of departure. We leave as a topic of future research a more thorough comparative analysis of all three approaches. We believe that such reflection may help us better address the privacy problems we experience as OSN users, regardless of whether we do so as activists or consumers.

## REFERENCE

- [1]. Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26 – 33, January/February 2005.
- [2]. J. Anderson, C. Diaz, J. Bonneau, and F. Stajano. Privacy-Enabling Social Networking over Untrusted Networks. In *ACM Workshop on Online Social Networks (WOSN)*, pages 1–6. ACM, 2009.
- [3]. Miriam Aouragh and Anne Alexander. The Egyptian Experience: Sense and Nonsense of the Internet Revolutions. *International Journal of Communications*, 5:1344 – 1358, 2011.





# International Journal of Ethics in Engineering & Management Education

Website: [www.ijee.in](http://www.ijee.in) (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

- [4]. F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In Privacy Enhancing Technologies Symposium, PETS 2011, volume 6794 of LNCS, pages 211–225. Springer, 2011.
- [5]. B. Berendt, O. Günther, and S. Spiekermann. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM* 48(4):101–106, 2005.
- [6]. E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Hummingbird: Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.
- [7]. A. Cuttillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine*, 47(12):94–101, 2009.
- [8]. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In USENIX Security Symposium, pages 303–320, 2004.
- [9]. FTC. Ftc charges deceptive privacy practices in google’s rollout of its buzz social network. Online, 03 2011.
- [10]. Glenn Greenwald. Hillary clinton and internet freedom. *Salon* (Online), 9. December 2011.

## About the Authors



**Dr. M.V.Siva Prasad**, Principal of Anurag Engineering College .He received B.E. [CSE] from Gulbarga University, M.Tech. [SE] from VTU, Belgaum and He was awarded Ph.D from Nagarjuna University, Guntur. He published number of papers in International & National journals. He

is a Life member of ISTE M.No. : LM 53293 / 2007. His research interests are Information Security, Web Services, Mobile Computing, Data mining and Knowledge.



**Ch.Suresh Kumar** received Master of Technology (Computer Science & Engineering) from Jawaharlal Nehru Technological University (JNTUH).My research interests include Information Security, Web Services, Cloud Computing, Data Mining and Mobile Computing. Anurag Engineering College (AEC),

Ananthagiri(V), Kodad (M), Nalgonda (Dt.), Andhra Pradesh, India.



**V.Ramya** Pursuing Master of Technology (Computer Science & Engineering) from Jawaharlal Nehru Technological University (JNTUH). B.Tech(IT) from Jawaharlal Nehru Technological University (JNTUH), In Anurag Engineering College (AEC), Ananthagiri (V), Kodad (M), Nalgonda(Dt.), Andhra Pradesh, India. My research interests include

Information Security, Web Services, Cloud Computing, Data Mining and Mobile Computing.