TWO TALES OF PRIVACY IN ONLINE SOCIAL NETWORK

Jagadeesh Kumar Surisetti, Miss G.Keerthana, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT
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 complementarity, and to identify potential integration challenges as well as research questions that so far have been left unanswered.

I. INTRODUCTION

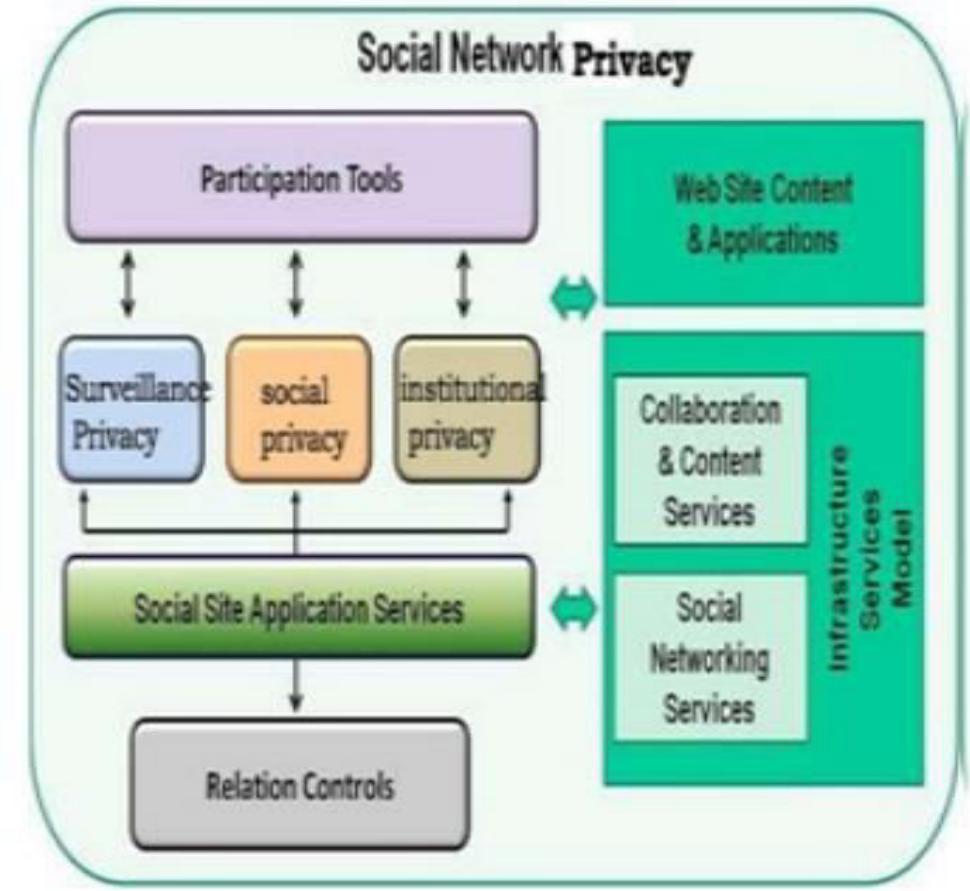
Can users have reasonable expectations of privacy in Online Social Networks (OSNs)? Media reports, regulators and researchers have replied to this question affirmatively. Even in the "transparent" world created by the Facebooks, LinkedIns and Twitters of this world, users have legitimate privacy expectations that may be violated. 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. 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"

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data 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. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

IV. 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".

V. IMPLEMENTATION

Number of Modules

After careful analysis the system has been identified to have the following modules:

1. **The Social Privacy Module**
2. **Surveillance Module**
3. **Institutional Privacy Module**
4. **Approach To Privacy As Protection Module**

1.The Social Privacy Module:

Social privacy relates to the concerns that users raise and to the harms that they experience when technologically mediated communications disrupt social boundaries. The users are thus "consumers" of these services. They spend time in these (semi-)public spaces in order to socialize with family and friends, get access to information and discussions, and to expand matters of the heart as well as those of belonging. That these activities are made public to 'friends' or a greater audience is seen as a crucial component of OSNs. In Access Control, solutions that employ methods from user modeling aim to develop "meaningful" privacy settings that are intuitive to use, and that cater to users' information management needs.

2.Surveillance Module:

With respect to surveillance, the design of PETs starts from the premise that potentially adversarial entities operate or monitor OSNs. These have an interest in getting hold of as much user information as possible, including user-generated content (e.g., posts, pictures, private messages) as well as interaction and behavioral data (e.g., list of friends, pages browsed, 'likes'). Once an adversarial entity has acquired user information, it may use it in unforeseen ways – and possibly to the disadvantage of the individuals associated with the data.

3.Institutional Privacy Module:

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.

4.Approach To Privacy As Protection Module:

The goal of PETs ("Privacy Enhancing Technologies") in the context of OSNs is to enable individuals to engage with others, share, access and publish information online, free from surveillance and interference. Ideally, only information that a user explicitly shares is available to her intended recipients, while the disclosure of any other information to any other parties is prevented. Furthermore, PETs aim to

enhance the ability of a user to publish and access information on OSNs by providing her with means to circumvent censorship.

VI. CONCLUSION

By juxtaposing 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.

REFERENCES

[1] Face book Developers. http://developers.facebook.com/.
[2] Face book Privacy Policy. http://www.facebook.com/policy.php/.
[3] Face book Statistics. http://www.facebook.com/press/info.php?statistics.
[4] Google+ Privacy Policy. http://http://www.google.com/intl/en/+/policy/.
[5] Open Social Framework. http://code.google.com/p/opensocial-resources/.
[6] The Google+ Project. https://plus.google.com.
[7] A.Besmer and H. Richter Lipford. Moving beyond untagging: Photoprivacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563–1572. ACM, 2010.
[8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web, pages 551–560. ACM, 2009.
[9] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pages 231–240. IEEE, 2011.
[10] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.