RESEARCH ARTICLE OPEN ACCESS

A Privacy Based Two Tales Over Online Social Networks

Datta V. Gunjal [1], Kavita U. Rahane [2]
M.E Research Scholar [1], Assistant Professor [2]
Department of Computer Science and Engineering
AVCOE Sangamner
India

ABSTRACT
Privacy being the main issue in social networking site. We all are users of such social networking sites. Facebook, Twitter, LinkedIn, E-mail, and Blogging such site's popularity is increasing day by day. Though, to protect the personal data of each user, these sites have their own privacy policies now it is necessity to have user level privacy policy. In this paper, we are trying to specify the problem regarding privacy and how privacy can also be achieved at user level.
***Keywords*:-** Surveillance privacy, Social privacy, Institutional privacy.

I. INTRODUCTION

The whole world is now become single community due to evolution of network and its different communicating fragments. Social Networking Sites (SNS) are like interface for such communicators. Social Networking Sites playing the role of virtual community that communicates world spreaded, like minded, friends, groups, business people. Due to its changing, improving, latest features like multimedia messages, gaming, and quizzes people are always connected and prefers to use these sites. It is an enormous network that made world more closely. Twitter, LinkedIn are used by professional users and followers like us are following them. Facebook, e-mail are more popular as they used casually.

Ultimately, along with its benefits it also has problem regarding privacy. People are giving their personal details like photos, birth date, comments, job, group membership, friends list, etc. If anyone is not aware about the privacy, then any unknown person can access your different personal information. Though, the site that you are using to communicate provides the privacy policies, sometimes it is also not sufficient to fully protect your account from stranger and your confidentiality may lost.

It is a little option that we are specifying here to secure your account on being SNS, and maintaining confidentiality. In this paper, we are first giving existing privacy types, their details, how privacy issued while communicating and eventually how we can resolve it.

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 Facebook, twitters etc. expectations that may be violated, researches the computer science tackle many problems arise in OSN that includes software tools and design principle to address OSN privacy issues.[9],[1] This solution is developed with the specific type of user, use and privacy problem in mind we now have a broad spectrum of approaches to tackle the complex privacy problems of OSNs. 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.[5]Three types of privacy problem has been distinguished that researchers in computer science will 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. 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.

A .Disadvantage

• Increases the risk of people falling prey to online scams that seem genuine, resulting in data or identity theft.

• Potentially results in negative comments from employees about the company or potential legal consequences if employees use these sites to view objectionable.

• Opens up the possibility for hackers to commit fraud and launch spam and virus attacks.

III. 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 inter-actions 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".

A. Advantage

• With Open Social, a third-party application can only query a user's friend data if both parties (user and friend) have consented and installed the application.

• The other major advantage is a subtle difference in policy between Facebook and Open Social.

B. Problem Statement

We argue that these different privacy problems are en-tangled, and that OSN users may benefit from a better integration of the three approaches. For example, consider surveillance and social privacy issues. OSN providers have access to all the user generated content and the power to decide who may have access to which information. This may lead to social privacy problems, e.g., OSN providers may increase content visibility in unexpected ways by overriding existing privacy set-tings. Thus, a number of the privacy problems users experience with their "friends" may not be due to their own actions, but instead result from the strategic de-sign changes implemented by the OSN provider. If we focus only on the privacy problems that arise from misguided decisions by users, we may end up deemphasizing the fact that there is a central entity with the power to determine the accessibility and use of information.

C. Scope

The first difference between the approaches lies in the way they treat explicit and implicit data disclosures. In the social privacy perspective, the privacy problems are associated with boundary negotiation and decision making. Both aspects are concerned with volitional actions, i.e., intended disclosures and interactions. Consequently, user studies are more likely to raise concerns with respect to explicitly shared data (e.g., posts, pictures) than with respect to implicitly generated data e.g., behavioral data). In contrast, PETs research is mainly concerned with guaranteeing concealment of information to unauthorized parties. Here, any data, explicit or implicit, that can be exploited to learn some-thing about the users is of concern. Shedding light on users' perception of implicit data may benefit both approaches. Studies showing how far users are aware of implicitly generated data may help better understand their privacy practices. The results of such studies may also provide indicators for how PETs can be more effectively deployed. If users are not aware of implicit data, it may be desirable to explore designs that make implicit data more visible to users.

IV. ACCOUNT OF EVENTS OF PRIVACY

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

- ✓ The Social Privacy Module
- ✓ Surveillance Module
- ✓ Institutional Privacy Module
- ✓ Approach to Privacy as Protection Module

A. 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 meth-ods from user modeling aim to develop "meaningful" privacy settings that are intuitive to use, and that cater to users' information management needs.

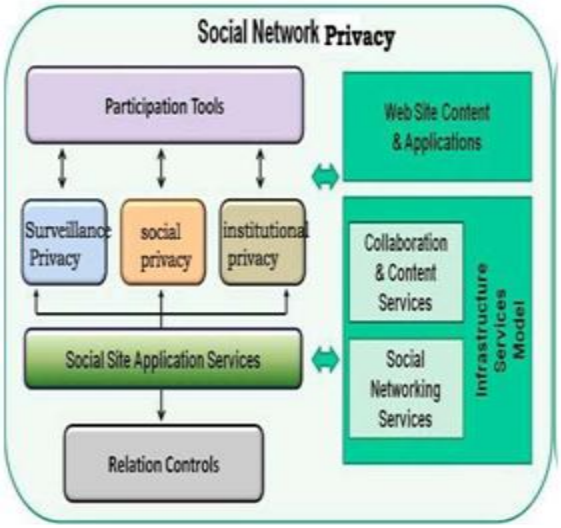

Fig1. Social Network Privacy

B. 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.

C. 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.

D. 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.

V. ALGORITHM FOR PRIVACY

1. Identify logged in user id
2. Identify user id of visiting profile page as visited
3. Identify friends of logged in user and store in Graph F
4. Identify friends of accessed user and store in Graph FN
5. for each node n in graph F
6. Initialize not_noisy = false
7. for each node m in graph FN
8. if (n == m) then
9. add n to valid_list
10. not_noisy = true
11. break
12. end if
13. end for
14. if (not_noisy == false)
15. add n to noisy_list
16. end if
17. end for
18. Reject noisy_list nodes
19. Initialize number_of_friends =count(F)
20. Initialize Probability = count(valid_list)/number_of_friends
21. if probability >0.5 then
22. for each label l in profile of logged in user
23. for each label k in profile of accessed user
24. if (l==k and type(l) == insensitive and type(k) == sensitive) then
25. add l to hide_list
26. end if
27. end for
28. if (empty(hide_list)) then
29. Display all sensitive labels
30. else
31. Display all details - hide_list
32. end if

VI. DISCUSSION

Each community of researcher's abstracts away some of the complexity associated with the OSN privacy problem through their framing, in the same way as we abstracted away institutional privacy in this article. Given the complexity of addressing privacy in OSNs, this is a necessary step to break down the problem into more graspable parts. The issue is, however, that the surveillance and social privacy approaches may actually have come to systematically abstract each other away. As a result, even though they speak about the same phenomenon, i.e., privacy in OSNs, they end up treating the surveillance and social privacy problems as independent of each other. We argue that given the entanglement between surveillance and

social privacy in OSNs, privacy research needs a more holistic approach that benefits from the knowledge base of the two perspectives. Specifically, we find that the approaches tend to answer the following questions differently: who has the authority to articulate what constitutes a privacy problem in OSNs? How is the privacy problem in OSNs articulated? Which user activities and information in OSNs are within the scope of the privacy problem? What research methods should be used to approach privacy problems in OSNs? What types of tools or design principles can be used to mitigate the issues associated with OSN privacy problems and why? How should these tools and design principles be evaluated?

In the following, we overcome some of the questions mentioned above: namely, the who, the how and the scope. We believe that a more thorough analysis of the different answers will pave the way to a possible integration of the two perspectives and to a more comprehensive approach to addressing users‟ privacy problems in OSNs. A. Who has the authority to articulate the privacy problem? While in PETs research "security experts" articulate what constitutes a privacy problem, in HCI, it is the "average OSN user" who does so. With PETs, the emphasis is on the privacy risks that may arise when adversaries exploit technical vulnerabilities: this puts the security experts in the driver's seat. This has positive and negative consequences. On the positive side, expertise in analyzing systems from an adversarial viewpoint is key to understanding the subversive uses of information systems; be it their repurposing for surveillance or the circumvention thereof. On the negative side, by formulating the problem as a technical one, the researchers bracket out the need to consider social and political analyses of surveillance practices. This introduces the risk of over-relying on techno-centric assumptions about how surveillance functions and what may be the most appropriate strategies to counter it. Moreover, the focus on improving security guarantees and on designing tools that behave predictably in every context inevitably plays down the importance of the social context and the users‟ talents in subverting technical boundaries in unexpected ways. It also deemphasizes the importance of considering the difficulties users may face in integrating these tools into their everyday life. In social privacy research, individual users are the actors articulating privacy concerns.

This research makes evident that technologies are open-ended: their use in practice may differ from the use cases devised by the designers. However, the focus on contextual practices inevitably results in small intensive studies. Surveys have a greater reach, but they have in common with small studies a focus on the perceptions and concerns of individual users. Hence, such studies do not provide much insight into collective privacy practices of established OSN communities, e.g., specific interest groups. Moreover, while user studies explore the correlations between demographics and privacy concerns, they rarely consider surveillance practices and how they may shape the privacy problem for specific populations. For example, underprivileged groups that are subject to greater surveillance may have other (social) privacy problems. This may require examining other demographic criteria in user studies, e.g., immigrants or lower income communities. Further, most of the studies are done with users in North America and Europe; few consider the needs of users elsewhere. How is the privacy problem articulated?

Who has the authority to articulate the privacy problem inevitably determines how these problems are defined. In the two approaches, it determines whether privacy problems are mapped to technology-induced risks or to the harms perceived by users. Users intuitively recognize causality when their OSN activities lead to concrete harms in interpersonal relationships. However, they cannot be reasonably expected to articulate concerns with respect to the more "abstract" privacy risks, derived from surveillance that often motivate the need for PETs. These may be risks that affect parts of the OSN population. Other abstract risks affect society as whole rather than individual users. For example, the greater intrusion in the private life of citizens that is enabled by OSN surveillance may result in an erosion of basic rights and freedoms. Often, even the experts struggle to articulate how the abstract risks associated with OSN surveillance may materialize into actual harms. In practice, it may even be impossible to establish the link between personal data disclosures and their ultimate consequences.

This is because the decision making processes of the organizations holding the data are complex and opaque. These processes involve multiple entities and sources of data, as well as sophisticated data processing algorithms. PETs designers can only guess which data is collected and how it could be exploited to the disadvantage of the user. Without information on actual OSN surveillance practices, it is hard to establish the capabilities and objectives of the adversaries, or the accuracy of the risk analysis. In such cases, the researchers prefer to study „worst case scenarios‟. While this is technically sensible, it may not reflect the most pressing practical concerns posed by surveillance. In social privacy, one challenge lies in determining the appropriate mechanisms through which OSN users can be exposed to complex and opaque privacy issues. This may empower users to find their positions on matters that do not seem to directly impact them. How to conduct studies that surface the user perspective on abstract risks and harms remains however an open question.

The first difference between the approaches lies in the way they treat explicit and implicit data disclosures. In the social privacy perspective, the privacy problems are associated with boundary negotiation and decision making. Both aspects are concerned with volitional actions, i.e., intended disclosures and interactions. Consequently, user studies are more likely to raise concerns with respect to

explicitly shared data (e.g., posts, pictures) than with respect to implicitly generated data (e.g., behavioral data). In contrast, PETs research is mainly concerned with guaranteeing concealment of information to unauthorized parties. Here, any data, explicit or implicit, that can be exploited to learn something about the users is of concern. Shedding light on users‟ perception of implicit data may benefit both approaches. Studies showing how far users are aware of implicitly generated data may help better understand their privacy practices. The results of such studies may also provide indicators for how PETs can be more effectively deployed. If users are not aware of implicit data, it may be desirable to explore designs that make implicit data more visible to users. The content of the data shared by the user with trusted entities is out of the scope of PETs. Researchers only consider the disclosure of data with respect to the "adversary", and PETs offer no protection to data disclosures made at the discretion of the user, e.g., to "trusted friends".

Further, the actual semantics of the data shared by the user are also out of the scope. Social privacy studies however reveal that the privacy concerns of users include the semantics of intentional data disclosures towards "trusted friends". This point to a possibly irreconcilable difference between the two approaches concerning what "privacy" actually entails. The two approaches have a fundamentally different take on censorship. In PETs research, privacy technologies are often instrumental for free speech and eluding censorship. They can enhance the user's ability to express themselves shielded from pressure by peers and authorities. PETs can conceal who is speaking and what is being said in a content-agnostic manner. On the other hand, in social privacy self-censorship is explored as a strategy. For example, some solutions aim to avoid regrettable disclosures by cautioning users when they are about to disclose sensitive content. Privacy practices are hence associated with silence as much as with expressing oneself. This raises the question of who has the authority to decide on the norms that underlie privacy nudges. There are situations in which OSN providers make certain actions invisible in order to avoid conflict, e.g., in Facebook users are not informed when their friends delete their relationship. These norms set by OSN providers enable certain interpersonal negotiations but disable others. This begs a greater question that is missing in social privacy research and that is only partially addressed with PETs: what can we offer users to enhance their ability to say what they want – including expressions that contest design, as well as social norms?

VII. CONCLUSION

By describing together 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] 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.

[2] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[3] Two Tales of Privacy in Online Social Networks. IEEE Security and Privacy Vol: PP No: 99 Year 2013.

[4] Improving Security and Efficiency in Attribute-Based Data Sharing. Volume 3 Issue 1, January 2014.

[5] E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams.Humming bird: Privacy at the time of twitter.IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

[6] 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.

[7] B. Berendt, O. G¨unther, and S. Spiekermann. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM, 48(4):101–106, 2005.

[8] A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, 47(12):94–101, 2009.

[9] Fred Stutzman and Woodrow Hartzog. BoundaryRegulation in social media. In CSCW, 2012.

[10] Kate Raynes - Goldie. Privacy in the Age of Facebook: Discourse, Architecture, Consequences. PhD thesis, Curtin University, 2012.

[11] Irma Van Der Ploeg. Keys To Privacy. Translations of "the privacy problem" in Information Technologies, pages15–36. Maastricht: Shaker, 2005.

[12] Glenn Greenwald. Hillary clinton and internet freedom. Salon (Online), 9. December 2011.