IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Two Tales of Privacy on Online Social Network

Amitha Varsha. R[1], Jeba Moses. T[2]

[1]B.Tech IT final year, IFET College of Engineering, Villupuram

[2]M.Tech, MISTE, Assistant Professor, Department of Information Technology, IFET College of Engineering, Villupuram

ABSTRACT

Privacy is one of the points that emerges when communication get mediated in Online Social Networks (OSN) different privacy problems have been emerged in the online social network ,this paper explains about the privacy in online social network about how to protect the personal information ,sensitive data , photos etc. .from the hackers or the unknown person, three approaches are used for privacy they are social network , surveillance and privacy. 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.

INDEX TERMS: *Online Social Network, Surveillance problem, Social, Institutional*

I. INTRODUCTION

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. NARRATIVES OF PRIVACY AND PRIVACY RESEARCH

A .The surveillance perspective

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. Governments also acknowledged that these new internet-based services could engage a public towards the exercise of their rights and basic freedoms based companies, for fundamental rights around the globe techno-deterministic framing of social media, and more specifically of OSNs, attracted a variety of cautionary reviews of the events. "Tweets were sent. Dictators were toppled. Internet = Democracy OSNs have acquired importance beyond the "social"[4], as a site for citizens to contest their ruling institutions., they render a very classical definition of privacy relevant in the context of OSNs [4].

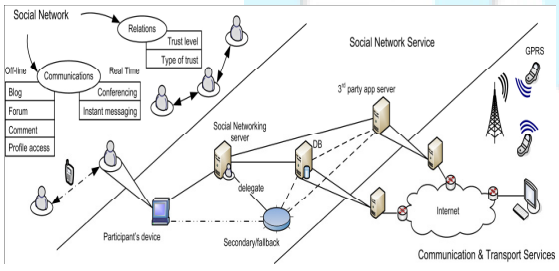

Fig 1: ARCHITECTURE DIAGRAM FOR ONLINE SOCIAL NETWORK

B. The social privacy perspective

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.

The goal of PETs [4],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.

The emphasis of PETs is thus on preventing (or at least limiting) the disclosure of user information, with the assumption that controlling how information is used after disclosure is impossible. The difficulty of control after disclosure is best For example, in the last years, Facebook introduced multiple changes to the privacy settings interface and added new features

(e.g., Newsfeed) that increased the availability of user information irrespective of their settings..these incidents underscore that, in practice, configuring the privacy settings is a symbolic act that does not provide users with effective control over the visibility of their information.

Similar privacy goals inspire Hummingbird [6], a variant of Twitter that implements several cryptographic protocols to "protect tweet contents, hash tags and follower interests from the (potentially) prying eyes of the centralized server". solutions require more radical changes to the system architecture while still relying on a centralized server for storing the data and guaranteeing its availability.

C. Privacy as expectations, decision making, and practice

Scholars in Human Computer Interaction (HCI) and Access Control have taken up the challenge of tackling social privacy in OSNs. In this research, the privacy problems users face are investigated through qualitative and quantitative studies. The users are consumers of OSN services whose concerns may show variety depending on demographics like gender, age, education, urbanity and technical skills. Specifically, contextual feedback mechanisms may aid users in making better disclosure decisions. These feedback mechanisms, also called privacy nudges, can help users to become aware of and overcome their cognitive biases.

To counter some of these problems, researchers have proposed corrective feedback mechanisms as well as a number of interface improvements to current privacy settings. In one solution, users are able to view their effective permissions as they change their privacy settings

Another major problem is that users encounter great difficulties to effectively configure their privacy settings. In order to successfully use their settings, users need to first locate them and understand their semantics. The response from the access control community, informed by research in user modeling, has been to develop privacy settings that are more expressive and closer to the users' mental models of OSNs. A number of the proposed access control models leverage users' 'attributes'. These attribute such as relationship ,roles and contextual information

III. DISCUSSION

We showed in the previous sections that the two approaches 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. 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. A first step for developing such a holistic approach lies in juxtaposing their differences. In doing so, we can understand the ways in which they are complementary as well as identify where the gaps lie. Specifically, we find that the approaches tend to answer the following questions differently:

A) who has the authority to articulate what constitutes a privacy problem in OSNs?
B) how is the privacy problem in OSNs articulated?
C) which user activities and information in OSNs are within the scope of the privacy problem?
D) what research methods should be used to approach privacy problems in OSNs?
E) what types of tools or design principles can be used to mitigate the issues associated with OSN privacy problems and why?
F) how should these tools and design principles be evaluated?

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 understand the subversive uses of information systems , 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.

B. How is the privacy problem articulated?

'Who' has the authority to articulate the privacy problems 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 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.

C. What is in the scope of the privacy problem?

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.

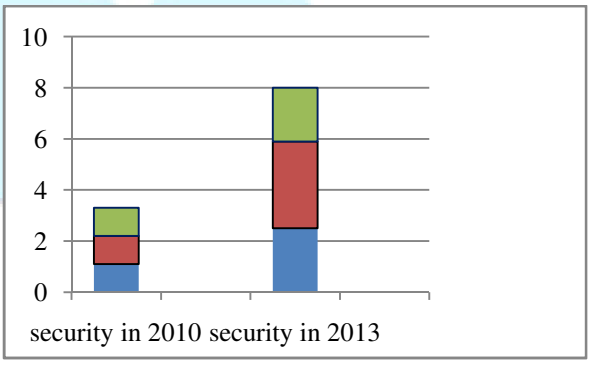

Fig 2: PERFORMANCE GRAPH

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

[4] 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.

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

[6] Leysia Palen and Paul Dourish. Unpacking ”privacy” for a networked world. In CHI ’03, pages 129 – 136, 2003.

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

[8] Rula Sayaf and Dave Clarke. Access control models for online social lnet works. In Social Network Engineering for Secure Web Data and Services. IGI - Global, (in print) 2012.

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

[10] Irma Van Der Ploeg. Keys To Privacy. Translations of “the privacy problem” in Information Technologies, pages 15–36. Maastricht: Shaker, 2005.

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

[12] Leysia Palen and Paul Dourish. Unpacking ”privacy” for a networked world. InCHI ’03, pages 129 – 136, 2003.