Analysing privacy issues in online social networks

Sk Rasheed[1], Guntapalli Minni[2]

[1] M.Tech (CS), Nimra College of Engineering and Technology, A.P., India.

[2]Associative Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering and Technology, A.P., India.

Abstract — Micro-blogging, as a form of social media, is fast emerging in recent years. Privacy is one of the friction points that emerges 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.

Keywords — OSN privacy problem, Surveillance, Social privacy, Institutional.

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 [1], [2].

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"[3].

Each of these approaches abstracts away some of the complexity of privacy in OSNs in order to focus on more solvable questions. However, researchers working from different perspectives differ not only in what they abstract, but also in their fundamental assumptions about what the privacy problem is. Thus, the surveillance, social privacy, and institutional privacy problems end up being treated as if they were independent phenomena. In this article, we argue that these different privacy problems are entangled, 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 settings. 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 design 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.

Similarly, surveillance problems are not independent of social privacy problems. Social practices in OSNs may have consequences for the effectiveness of intrusive surveillance measures. For instance, the social tagging of people in pictures, coupled with the use of facial recognition by OSN providers, increases the visual legibility of OSN users. This can be used for surveillance purposes, e.g., to identify unknown protesters in pictures taken at demonstrations. Further, it also decreases the protective function of simple obscurity measures like detagging oneself, something consumers of OSNs often utilize as a privacy protection strategy. This shows that how social privacy problems are managed can directly impact the power relationships between users and OSNs.

The entanglement of surveillance and social privacy explored in this paper is easily extended to institutional privacy. 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. However, when researchers tackle institutional privacy they again do so as if it were a problem independent of the other two.

II. Related work

In 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. In the final section, we juxtapose their differences in order to understand their complementarity 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 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. For example, in institutional privacy solutions the service provider is trusted and law enforcement is a legitimate stakeholder. In the surveillance perspective however, these actors are likely "adversaries". Further, institutional privacy provides organization-centric solutions. Researchers do not however study how social privacy issues may reconfigure organizational data management specific to OSNs [4]. Most importantly, rarely do researchers across the three communities collaborate to address these divergences. While much advance has been made in addressing institutional privacy, since it is not specific to OSNs, we have chosen to leave it out of the scope of this work.

III. PROPOSED WORK

A. The surveillance perspective

For a long time, journalists, activists and researchers argued that that web based social media would deliver conditions for the emergence of politically engaged publics and democracy. The "Twitter" and "Facebook revolutions" seemed to confirm these beliefs. Causality between technology and political change was recognized in Moldova, Tunisia, Egypt, in the U.S. during the months that led to the presidential election of Barack Obama, and throughout the series of organized gatherings known as the Occupy Movement. Governments also acknowledged that these new internet-based services could engage a public towards the exercise of their rights and basic freedoms. In 2011, U.S. Secretary of State Clinton launched an initiative on "Internet Freedom" that embraced the importance of these services, run by U.S. based companies, for fundamental rights around the globe [5].

At first sight, these events spoke much truth to theories of social media as a driving force of political and social change. On a closer look, however, this 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. QED." started an article which regards such simplified accounts as a cyber-utopian delusion [6]. Other researchers urged for a more nuanced account of the events that recognizes the role of physical social networks and political organization [3]. Cyber-dystopians responded by pointing at reports on intelligence agencies around the world developing strategies for monitoring, blocking and leveraging OSNs for their own interests.

In its current day manifestations, state institutions assert such power in collaboration with private organizations, constituting what some authors call the "surveillant assemblage" [7]. This is exactly the type of surveillance that occurs when law enforcement and intelligence agencies around the world start acting in concert with OSN providers. Besides 'silently' conducting surveillance, these assemblages may act to limit free speech, e.g., by censoring user content or groups in OSNs. In other instances, state actors in collaboration with Internet Service Providers (ISPs) block OSN sites. This practice, which has become common in situations of civil unrest, aims to prevent citizens from leveraging OSNs to self-organize or share and access information

B. The social privacy perspective

In contrast to the surveillance perspective, when mainstream media report on privacy violations in "everyday life", they do not frame OSNs as incubators of social change, but as consumer goods. 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 greater audiences is seen as a crucial component of OSNs. However, it is important that revelations, and the interactions that follow, happen at the users' discretion. Otherwise users can be subject to "unexpected" and "regrettable" interactions with friends, family and employers.

Figure1: Social Network users and their relations

Popular accounts of privacy violations in news media have made this social privacy problem evident: partners finding out about wedding rings before the official proposal, employer's learning about deceitful sick leaves, tax authorities finding out about undeclared expensive purchases, and families discovering the sexual preferences of their children.

These privacy problems have been studied by a variety of research communities within and beyond computer science.

Researchers have shown that the way transparency, sharing and friending is embedded into OSN design plays an important role in the way information flows in these networked systems [8]. These novel flows of information may undermine the spatial and temporal assumptions that physical world communication depends on. Established boundaries that underlie social interactions may be disrupted while new ones may come into being. These may be boundaries between the private and the public, the intimate and the distant, openness and closeness as well as the self and others [9].

For example, a casual status update on an OSN may start living a life of its own. With one click, a user may reach a remarkable audience, while she may neither intend its size nor its geographic distribution. The reach of the status update may not only depend on her: her friends may decide to 'share' it further with others in their networks. Multiple copies of the update may hence exist much longer than the intended conversation blurb.

Social privacy relates to the concerns that users raise and to the harms that they experience when technologically mediated communications disrupt social boundaries. Numerous research studies show that OSN users grapple with a variety of related issues: damaged reputations, interpersonal conflicts, presentation anxiety, unwanted contacts, context collision, stalking, peer pressure, blackmailing, and the list continues. Palen and Dourish suggest addressing these issues by exploring design mechanisms and principles that enable users to establish appropriate "privacy practices" [10]. These are defined as those actions that users collectively or individually take to negotiate their boundaries with respect to disclosure, identity and temporality in technologically mediated environments. Further, enabling privacy practices through design requires expanding the focus from individual actions to include collective dynamics, and dispensing with the online-offline divide.

An important body of work addressing social privacy problems in OSNs comes from the HCI and Access Control communities. Research in HCI, often informed by behavioral economics, focuses on transparency and feedback solutions. The objective is to develop design principles that assist individual users in making better privacy decisions and hence improving collective privacy practices. 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.

IV. 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] FTC. Ftc charges deceptive privacy practices in google's rollout of its buzz social network. Online, 03 2011.

[2] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137– 1206, 2009.

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

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

[5] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137– 1206, 2009.

[6] Kevin D. Haggerty and Richard V. Ericson. The Surveillant Assemblage. British Journal of Sociology, 51(4):605 – 622, 2000.

[7] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proceedings of the 28th international conference on Human factors in computing systems, CHI '10, pages 1111–1114, New York, NY, USA, 2010. ACM.

[8] Evgeny Morozov. Facebook and Twitter are just places revolutionaries go. The Guardian, 11. March 2011.

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

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