IEEE SECURITY AND PRIVACY VOL:PP NO:99 YEAR 2013

# Two tales of privacy in online social networks

Seda Gürses and Claudia Diaz
KU Leuven ESAT/COSIC, iMinds
Email: firstname.secondname@esat.kuleuven.be

***Abstract*—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.**

## 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 [9], [11].

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" [17].

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 de-tagging 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

*This article has been accepted for publication at the IEEE Security & Privacy Magazine. This is the authors' version of the paper.*

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.

Research on institutional privacy is aligned with regulatory approaches to privacy, e.g., the Fair Information Practice Principles (FIPPs) recommended by the Federal Trade Commission (FTC) and the EU Data Protection Directive (EU DPD). Both FIPPs and the EU DPD strive to balance organizational and individual needs in data collection and processing: organizations should be able to collect, process and share personal data, and they should provide users with some transparency and control over the same – with a number of exceptions, e.g., for law enforcement. Computer science research on 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. 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 [15]. 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.

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. 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.

## II. Narratives of Privacy and Privacy Research

### 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 [10].

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 [14]. 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.

While the debates continue, two matters seem evident. First, OSNs have acquired importance beyond the "social", as a site for citizens to contest their ruling institutions. Second, those same institutions will attempt to instrumentalize OSNs to monitor and intervene in the lives of their citizens. These two uses, the citizens' use of OSNs for democratic emancipation and state institutions' reflex to monitor and influence those citizens, are in tension. In that sense, they render a very classical definition of privacy relevant in the context of OSNs: privacy as a right that citizens can invoke to protect themselves from an overbearing surveillant state [20].

What is re-occurring in OSNs with respect to surveillance and privacy is reflective of a tension at the core of the "western" modern state. The complexity of any modern state is managed through practices of individual identification, registration and classification. Yet, such surveillance practices, while necessary for the functioning of the bureaucracy, also increase such power of the state to encroach upon its citizens.

In its current day manifestations, state institutions assert such power in collaboration with private organizations, constituting what some authors call the "surveillant assemblage" [12]. 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.

Given the effectiveness and reach of the Internet, and the track record of surveillant assemblages, some privacy researchers consider that it may not be sufficient to rely solely on the legal measures to protect their citizens. They thus propose solutions that counter such surveillant assemblages through another type of code: software itself. This is one of the anchor points for one set of technical privacy solutions, which we call "Privacy Enhancing Technologies" (PETs). We note that while the term 'PETs' is often used to describe a broad range of privacy solutions, here we use it in its narrowest sense, to refer to technologies specifically designed to protect citizens' online privacy towards overbearing states and collaborating service providers.

### *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.

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 [17]. 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 [16].

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" [16]. 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.

## III. Approaches to privacy in computer science

In the previous section we showed that both in media discourse, as well as in research, the surveillance and social privacy perspectives are treated as separate problems. Next, we turn our attention to the corresponding privacy research traditions in computer science. We give a short overview of some of their assumptions, definition of the privacy problem, methods, objectives, and proposed solutions.

### *A. Privacy as protection from surveillance and interference*

The set of technologies that we refer to as "Privacy Enhancing Technologies" (PETs) grew out of cryptography and computer security research, and are thus designed following security engineering principles, such as threat modeling and security analysis. Classical security technologies were developed for national security purposes, and later, for securing commercial information and transactions. They were meant to protect state and corporate secrets, and to shield organizational operations from disruptions. The privacy problems addressed by PETs are in many ways a reformulation of old security threats, such as confidentiality breaches or denial of service attacks. This time however, ordinary citizens are the intended users of the technologies, and surveillant assemblages are

the threatening entities from which they need protection. Unsurprisingly, the quintessential user and use of PETs is the 'activist' engaged in political dissent.

The goal of PETs 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.

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.

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 illustrated by OSN "privacy settings". Privacy settings allow users to express their preferences with respect to the revelation and concealment of their data. These settings, however, typically do not contain options for hiding the information from the OSN provider itself, who by design has access to the information of all users. Further, users rely on the OSN provider for enforcing their settings, which introduces additional risks. 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.

Instead of relying on the provider to enforce privacy settings, PETs leverage cryptography so that users themselves have the ability to prevent unwanted disclosures. Solutions in this space include browser plug-ins such as Scramble! [4] Scramble! allows users to specify the set of friends designated as the "intended audience" of a status update or comment. The content is encrypted prior to being shared in the OSN, so that only friends who are part of the "intended audience" are able to decrypt it. The use of cryptography ensures that the content is not disclosed to OSN providers or other third parties, curtailing their ability to perform surveillance. Furthermore, if the OSN provider fails to respect the user's settings, only encrypted information is revealed to other (unauthorized) OSN users.

Similar privacy goals inspire Hummingbird [6], a variant of Twitter that implements several cryptographic protocols to "protect tweet contents, hashtags and follower interests from the (potentially) prying eyes of the centralized server". Other solutions require more radical changes to the system architecture while still relying on a centralized server for storing the data and guaranteeing its availability. In the proposal by Anderson et al. [2] the central server is reduced to a data store to which users upload blocks of encrypted data containing their posts, pictures, friend lists, etc. As in the two previous examples, only authorized friends (who have the necessary decryption keys) are able to access the data.

While cryptography preserves the confidentiality of the user-generated content uploaded to the OSN, it does not conceal user interactions and behavior. Additional strategies, such as the use of dummy traffic, are necessary to obscure user activity and prevent the adversary from gaining intelligence through the analysis of implicit (traffic) data.

Some researchers propose implementing the OSN as a distributed architecture. The objective is to eliminate the need for a central server that is in a privileged position to observe all the activity in the OSN, and which constitutes a "single point of failure" with respect to service and data availability. One such proposal is Safebook [7], a peer-to-peer based OSN design that aims to conceal friendship links, as well as user data and interactions, towards adversaries with a limited view of the network.

Besides protection from surveillance, PETs also aim to provide users with means to circumvent censorship. Service providers have the power to confine the users' freedom to express themselves and access information. For example, OSN providers may police user-generated content, while ISPs can make OSN sites inaccessible. The use of cryptography to conceal user content limits the OSN providers' ability to censor information shared in the network, as they can no longer examine user content and make a judgement on its "appropriateness". With respect to the blocking of OSN websites, PETs solutions include anonymous communication networks such as Tor [8]. Although Tor is a general-purpose (rather than OSN specific) solution, its role in social media censorship circumvention during the Arab Spring and Iran's Green Movement has been widely recognized. The key feature of Tor is that when users connect through it, ISPs cannot determine the destination of the users' communications – and thus their capacity to selectively block websites is undermined.

We further note that PETs are content-agnostic with respect to surveillance as well as censorship, i.e., the semantics of what OSN users actually talk about are left out of the scope. This contrasts with the social privacy perspective introduced next, where the semantics of user content, and its reception in a social context, are part of the privacy problem.

While several content protection (encryption) plug-ins for OSNs have been implemented as research prototypes, none has been adopted by a significant user base. Many factors are pointed out as explaining the lack of adoption of these solutions, including problems with usability, bootstrapping, network effect, etc. Moreover, the concealment of user-generated content towards the OSN provider is in direct conflict with OSN business models based on personalized advertising. Thus, should these solutions gain popularity, it is an open question

whether OSN providers would tolerate their use within their platforms.

### B. Privacy as expectations, decision making, and practice

Scholars in Human Computer Interaction (HCI) and Access Control (we restrict ourselves to research on user-centric access control at the intersection of HCI and User Modeling – there is greater body of work on OSN access control models that focuses on the formal properties of these rather than on user needs) 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. The results of these studies help to explore design mechanisms and principles that enable users to establish appropriate privacy practices.

In HCI research it is assumed that technical solutions that equate privacy with concealment are too rigid to accommodate the users' practices. Information concealment does not necessarily imply privacy, and disclosure is not inevitably associated with (undesirable) accessibility. Daily practices, such as making explicit that you do not want to be disturbed, illustrate that a disclosure can be used to negotiate privacy boundaries. Further, studies show that users develop their own strategies to maintain their privacy and manage their identity while benefiting from participating in OSNs. For example, some users create multiple accounts at a given service. These may be pseudonymous, obscured or transparent accounts [19]. While these 'obscured' profiles may not conceal the users' profile effectively, users find that the protections they offer are sufficient for their daily needs.

Researchers perform user studies that are contextualized and are conducted iteratively. These studies observe how, given an OSN design, users negotiate and reconfigure their social boundaries. Hence, this research avoids focusing on one-off disclosure and concealment decisions without contextualization. Further, the researchers explore whether and how practices change when privacy design principles are applied by iterating user studies with enhanced prototypes.

In addition to studying privacy practices, researchers have focused on the role of decision making in social privacy problems. A number of studies in behavioral economics point to failures in individual or social decision-making as the source of many social privacy problems in OSNs. These show that users systematically fail to correctly estimate privacy risks [1] and to match their privacy preferences to their actual behaviors [5]. These failures motivate the exploration of design mechanisms that aid users in making better privacy decisions – especially when they lack complete information, are subject to cognitive and behavioral biases, and are uncertain with respect to the outcomes of their decisions.

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. For example, if the users are experiencing harms or regrets with respect to emotional outbursts, they can be sent alerts before posting messages that use emotional language [21]. Such feedback can be used to trigger reflection and self-censorship, instead of the desire for immediate gratification through disclosure.

Users may also negotiate their boundaries by "skillfully" using their OSN privacy settings. However, there are major problems associated with privacy settings. A variety of decision-making problems re-appear when users utilize their OSN privacy settings. Users may be subject to social influence or may fail to predict future preferences. They may have a tendency to compromise in the present in order to get immediate gratification. In other cases, users may give greater prevalence to not-so-close friends (weak ties) and may experience difficulty in estimating trust towards these. All in all, given the multitude of decisions, users may simply experience cognitive overload.

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 addition to decreasing the cognitive load of the user, these solutions aspire to make the potential effects of an action more visible in context. In one solution, users are able to view their effective permissions as they change their privacy settings [13].

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. Further, the settings need to be at a meaningful granularity to express the users' disclosure preferences.

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 attributes, e.g. relationships, roles, or other contextual information, can be used to aid users in configuring their settings to express their actual preferences. Other models propose using artificial intelligence to assist users in keeping their privacy settings up to date [18].

User studies have been successfully leveraged to rethink social privacy and its evolution with OSN design. These studies have made the importance of the user factor visible to other privacy researchers, to policy makers and to regulators. Even further, some of their results have already found an audience in commercial OSNs. This illustrates that, in contrast to solutions developed to address surveillance concerns, the emphasis on OSN 'consumers' aligns well with the incentives of companies to design systems that are comfortable for their customers.

## IV. Discussion

We showed in the previous sections that the two approaches frame and address the OSN privacy problem very differently. Each community of researchers 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. 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:

- 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 tackle 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. For example, it is unclear if a study focused on activists or users in contexts with limited ICT access would surface the same privacy concerns. Conducting such studies remains however extremely challenging: researchers do not always have easy access to these groups of users, and the design of the studies would need to take into account their specific socio-political context.

Finally, as OSNs become integrated into everyday life, users tend to take them as a given, and are likely to report on how they make do with the given design. This further constrains what can be discovered through user studies. For example, a study that asks users to critically engage in the values and ideologies embedded into a particular OSN design, or to imagine radical design alternatives, may overwhelm participants and fail to provide results. In order to address this limitation, we may have to introduce other methods, e.g., workshops in which experts explore designs together with users.

### 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.

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. For example, users deemed as not fitting societal 'norms' may be discriminated or repressed as a result of inferences made from their data. Other abstract risks affect society as a 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.

For example, studies have shown that friendship relations in OSNs can be analyzed to infer sensitive personal preferences, such as sexuality and political orientation, even if the users have not disclosed this information. The inferred preferences may or may not be correct, and we do not know if OSN providers employ such inference mechanisms. If they do employ them, we do not know which decisions are made based on them, or who else has access to the inferences.

Understanding how decisions are made on the basis of which data, however, would require access to algorithms and management decisions that are typically not available for scrutiny by either users or independent experts. The opacity of OSN providers poses an enormous challenge to both research in PETs and in social privacy.

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.

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

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 points 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, e.g., who decides what constitutes sensitive content?

Finally, users may benefit from being able to question norms asserted through design. 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?

## V. Conclusion and Future Work

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.

*Acknowledgments*

This work was supported in part by the projects: IWT SBO SPION, FWO G.0360.11N, FWO G.0686.11N, and GOA TENSE (GOA/11/007).

## REFERENCES

[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.

[4] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In *Privacy Enhancing TechnologiesSymposium, 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. 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.

[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.

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

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

[13] 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.

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

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

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

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

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

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

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

[21] Yang Wang, Saranga Komanduri Pedro Giovanni Leon, Gregory Norcie, , Alessandro Acquisti, and Lorrie Faith Cranor. "I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook. In *Symposium on Usable Privacy and Security*, 2011.