Two Tales of Privacy in Online Social Networks

Seda Gürses and Claudia Diaz | KU Leuven

Different communities of computer science researchers have framed the online social network (OSN) privacy problem as one of surveillance, institutional privacy, or social privacy. In tackling these problems, researchers have treated them as if they were independent. However, OSN privacy research would benefit from a more holistic approach.

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 Facebook, LinkedIn, and Twitter, users have legitimate privacy expectations that could be violated.[1,2]

Researchers from different computer science disciplines have tackled some of the problems that arise in OSNs and propose a diverse range of privacy solutions, including software tools and design principles. 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 OSNs' complex privacy problems. At the same time, it has led to a fragmented landscape of solutions that address seemingly unrelated problems. Consequently, the field's vastness and diversity remain mostly inaccessible to outsiders and, at times, even to computer science researchers who specialize in a specific privacy problem. One of our objectives is to put these research approaches to OSN privacy into perspective.

OSN Privacy Problems

We distinguish the three types of privacy problems that computer science researchers typically tackle. The *surveillance* problem arises when governments and service providers leverage OSN users' personal information and social interactions. *Social privacy* problems emerge through the necessary renegotiation of boundaries as social interactions are mediated by OSN services. The third problem, *institutional privacy*, relates to users losing control and oversight of OSNs' collection and processing of their information.[3]

Each approach to these problems abstracts away some of the complexity of privacy in OSNs 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.

We argue that these different privacy problems are entangled and that OSN users would 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 has access to which information. This might lead to social privacy problems—for

example, OSN providers might increase content visibility in unexpected ways by overriding existing privacy settings. Thus, some of the privacy problems users experience with their "friends" might not be due to their own actions but instead result from the OSN provider's strategic design changes. If we focus *only* on the privacy problems that arise from users' misguided decisions, we might end up deemphasizing the fact that there's a central entity with the power to determine the accessibility and use of information.

Similarly, surveillance problems aren't independent of social privacy problems. OSN social practices might 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 OSN users' visual legibility. This can be used for surveillance purposes, for instance, to identify unknown protesters in pictures taken at demonstrations.[4] Furthermore, it decreases the protective function of simple obscurity measures such as untagging oneself—something OSN consumers often utilize as a privacy protection strategy toward their peers. However, untagging doesn't diminish the surveillance capabilities of OSN providers, who might keep a record of the tag as well as run facial recognition algorithms. This shows that the way social privacy problems are managed can directly impact the power relationships between OSN providers and users.

> **Researchers working from different perspectives differ not only in what they abstract but also in their fundamental assumptions about what the privacy problem is.**

This entanglement of surveillance and social privacy easily extends to institutional privacy as well. The way in which personal control and institutional transparency requirements (as defined through legislation) are implemented impacts 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.

Institutional privacy research aligns with regulatory approaches to privacy, for example, the Fair Information Practice Principles (FIPPs) recommended by the US Federal Trade Commission and the EU Data Protection Directive (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 should provide users with some transparency and control over the same—with several exceptions, such as for law enforcement. Computer science research on institutional privacy studies ways to improve organizational data management practices for compliance, for example, by developing mechanisms for information flow control and accountability in the back end.

The challenges 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. However, from the surveillance perspective, these actors are likely adversaries. Furthermore, institutional privacy provides organization-centric solutions. However, researchers don't study how social privacy issues might reconfigure organizational data management specific to OSNs.[5] Most important, researchers across the three communities rarely collaborate to address these divergences.

Many advances have been made in addressing institutional privacy. Some examples are studies on increasing the readability of privacy policies, automated matching of user and service provider privacy policies, and access control models that limit the processing of personal data to expressed purposes. However, because institutional privacy isn't specific to OSNs, we've chosen to leave it out of this article's scope.

Narratives of Privacy and Privacy Research

To contextualize computer science privacy research, we first look at the narratives that inform OSN surveillance and social privacy problems.

The Surveillance Perspective

For a long time, journalists, activists, and researchers argued 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, and Egypt; in the US during the months leading up 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 the public toward the exercise of their rights and basic freedoms. In 2011, US Secretary of State Hillary Clinton launched an "Internet Freedom" initiative that embraced the importance of these

services, run by US-based companies, for fundamental rights around the globe.[6]

At first sight, these events spoke much truth to theories of social media as a driving force of political and social change. However, on a closer look, 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" starts an article that regarded such simplified accounts as a cyberutopian delusion.[7] Other researchers urged for a more nuanced account of the events that recognized the role of physical social networks and political organization.[8] Cyberdystopians responded by pointing to reports on intelligence agencies around the world developing strategies for monitoring, blocking, and leveraging OSNs for their own interests.

Although 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 their citizens' lives. These two uses—citizens' use of OSNs for democratic emancipation and the state institutions' reflex to monitor and influence those citizens—are in tension. In that sense, they render a 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.[9]

What's occurring in OSNs with respect to surveillance and privacy reflects a tension at the core of the modern "Western" state. Any modern state's complexity is managed through practices of individual identification, registration, and classification. Yet, such surveillance practices, although necessary for bureaucratic function, also increase the state's power to encroach on its citizens.

In their current manifestations, state institutions assert such power in collaboration with private organizations, constituting what some authors call the *surveillant assemblage*.[10] This is the exact 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 might act to limit free speech, for example, by censoring user content or groups in OSNs. In other instances, state actors in collaboration with ISPs might block OSN sites. This practice, which has become common in situations of civil unrest, aims to prevent citizens from leveraging OSNs to self-organize and share and access information.

Given the Internet's effectiveness and reach and the surveillant assemblages' track record, some privacy researchers believe that relying solely on legal measures to protect citizens might not be sufficient. 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). Note that although the term is often used to describe a broad range of privacy solutions, we use it here in its narrowest sense to refer to technologies specifically designed to protect citizens' online privacy from overbearing states and collaborating service providers.

The Social Privacy Perspective

In contrast to the surveillance perspective, when mainstream media report on privacy violations in "everyday life," they don't frame OSNs as incubators of social change but as consumer goods. Users are thus consumers of these services. They spend time in these (semi-) public spaces to socialize with family and friends, get access to information and discussions, and gain a sense of belonging. That these activities are made public to friends or greater audiences is a crucial component of OSNs. However, it's important that revelations, and the interactions that follow, occur 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 engagement rings before the official proposal, employers learning about deceitful sick leaves, tax authorities finding out about undeclared expensive purchases, and parents discovering their children's sexual preferences.

A variety of research communities within and beyond computer science have studied these privacy problems. Researchers have shown that the way transparency, sharing, and friending is embedded into OSN design plays an important role in how information flows in these networked systems.[3] These novel information flows might undermine the spatial and temporal assumptions on which physical-world communication depends. Established boundaries that underlie social interactions might be disrupted while new ones might emerge. These boundaries might be between the private and the public, the intimate and the distant, openness and closeness, and the self and others.[11]

For example, a casual status update on an OSN might start living a life of its own. With one click, a user can reach a remarkable audience, while he or she might not intend its size or its geographic distribution. The reach of the status update might not only depend on this user: friends might decide to share it further with others in their networks. Multiple copies of the update might exist much longer than the intended conversation blurb.

Social privacy relates to the concerns that users raise and to the harms they experience when technologically mediated communications disrupt social boundaries. Numerous research studies show that OSN users grapple with a variety of related issues, including damaged reputations, interpersonal conflicts, presentation anxiety, unwanted contacts, context collision, stalking, peer pressure, and blackmailing.

Leysia Palen and Paul Dourish suggest addressing these issues by exploring design mechanisms and principles that let users establish appropriate *privacy practices*—those actions that users collectively or individually take to negotiate their boundaries with respect to disclosure, identity, and temporality in technologically mediated environments.[11] Furthermore, 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 human-computer interaction (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 improve collective privacy practices. In access control, solutions that employ methods from user modeling aim to develop intuitive, "meaningful" privacy settings that cater to users' information management needs.

Approaches to Privacy in Computer Science

To surface their scoping of the privacy problem and to see the characteristics in assumptions, methodologies, and objectives that distinguish them, we turn our attention to the corresponding privacy research traditions in computer science.

Privacy as Protection from Surveillance and Interference

The set of technologies that we refer to as PETs grew out of cryptography and computer security research and are thus designed using 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 PETs address are in many ways a reformulation of old security threats, such as confidentiality breaches or denial-of-service attacks. However, this time, ordinary citizens are the intended users of the technologies, and surveillant assemblages are the threatening entities from which they need protection. Unsurprisingly, the quintessential PETs user is the activist engaged in political dissent.

PETs' goal in the context of OSNs is to enable individuals to engage with others and share, access, and publish information online, *free from surveillance and interference*. Ideally, only information that users explicitly share is available to their intended recipients, while the disclosure of *any* other information to *any* other parties is prevented. Furthermore, PETs aim to enhance users' ability to publish and access information on OSNs by providing them with means to circumvent censorship.

With respect to surveillance, PETs' design starts from the premise that potentially adversarial entities operate or monitor OSNs. These entities have an interest in acquiring as much user information as possible, including user-generated content (for example, posts, pictures, and private messages) and interaction and behavioral data (for example, lists of friends, pages browsed, and likes). Once an adversary has acquired user information, it might use it in unforeseen ways—possibly to the disadvantage of the individuals associated with the data.

PETs' emphasis 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, which let users express their preferences with respect to their data's revelation and concealment. However, these settings typically don't contain options for hiding the information from the OSN provider, which by design, has access to all users' information. Furthermore, users rely on the OSN provider to enforce their settings, which introduces additional risks. For example, in the past few years, Facebook introduced multiple changes to the privacy settings interface and added new features (for example, newsfeed) that increased the availability of user information irrespective of privacy settings. These incidents underscore that, in practice, configuring privacy settings is a symbolic act that doesn't 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 can prevent unwanted disclosures. Solutions in this space include browser plug-ins such as Scramble!,[12] which lets a user specify the set of friends designated as a status update's or comment's intended audience. The content is encrypted prior to being shared in the OSN so that only friends who are part of the intended audience can decrypt it. The use of cryptography ensures that the content isn't 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, 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."[13] 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 Jonathan Anderson and his colleagues' proposal, the central server is reduced to a datastore to which users upload blocks of encrypted data containing their posts, pictures, friend lists, and so forth.[14,15] As in the two previous examples, only authorized friends (who have the necessary decryption keys) can access the data.

Although cryptography preserves the confidentiality of the user-generated content uploaded to the OSN, it doesn't 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 that constitutes a single point of failure with respect to service and data availability. One such proposal is Safebook, a peer-to-peer-based OSN design that aims to conceal friendship links and user data and interactions from adversaries with a limited view of the network.[16]

Besides protection from surveillance, PETs also aim to provide users with a means to circumvent censorship. Service providers have the power to confine users' freedom to express themselves and access information. For example, OSN providers might police user-generated content, whereas 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 judgment on its "appropriateness." With respect to the blocking of OSN websites, PETs solutions include anonymous communication networks such as Tor.[17] 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 is widely recognized. Tor's key feature is that when users connect through it, ISPs can't determine the destination of user communications—this undermines their capacity to selectively block websites.

We further note that PETs are content agnostic with respect to surveillance and censorship—that is, the semantics of what OSN users actually talk about are left out of the scope. This contrasts with the social privacy perspective in which the content semantics, and their reception in a social context, are part of the privacy problem.

Although several content protection (encryption) plug-ins for OSNs have been implemented as research prototypes, none have been adopted by a significant user base. Many factors contribute to the lack of adoption of these solutions, including problems with usability, bootstrapping, and network effects. Moreover, concealing user-generated content from the OSN provider directly conflicts with OSN business models based on personalized advertising. Thus, should these solutions gain popularity, it's an open question whether OSN providers would tolerate their use on their platforms.

Privacy as Expectations, Decision Making, and Practice

HCI and access control scholars have taken up the challenge of tackling social privacy in OSNs. (We restrict ourselves to research on user-centric access control at the intersection of HCI and user modeling—a greater body of work exists on OSN access control models, which focuses on formal properties of these rather than on user needs.) In this research, the privacy problems that users face are investigated through qualitative and quantitative studies. The users are consumers of OSN services whose concerns might show variety depending on demographics such as gender, age, education, urbanity, and technical skills. The results of these studies help us explore design mechanisms and principles that enable users to establish appropriate privacy practices.

From this perspective, technical solutions that equate privacy with concealment are too rigid to accommodate users' practices. Information concealment doesn't necessarily imply privacy, and disclosure isn't inevitably associated with undesired accessibility. Daily practices, such as making explicit that you don't 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 might be pseudonymous, obscured, or transparent accounts.[18] Although these obscured profiles might not effectively conceal a user profile, users find that the protections they offer are sufficient for their daily needs.

Researchers perform user studies that are contextualized and 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. Furthermore, 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[19] and to match their privacy preferences to their actual behaviors.[20] 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 about the outcomes of their decisions.

Specifically, contextual feedback mechanisms might aid users in making better disclosure decisions. These feedback mechanisms, also called *privacy nudges*, can help users become aware of and overcome their cognitive biases. For example, if users are experiencing harm or regret with respect to emotional outbursts, they can be sent alerts before posting messages that use emotional language.[21] Such feedback can trigger reflection and self-censorship, instead of the desire for immediate gratification through disclosure.

Users might also negotiate their boundaries by using their OSN privacy settings. However, major problems associated with privacy settings exist. Users might be subject to social influence or might fail to predict future preferences. They might have a tendency to compromise in the present to get immediate gratification. In other cases, users might experience difficulty in estimating trust toward not-so-close friends. All in all, given the multitude of decisions, users might 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 users' cognitive load, these solutions aspire to make the potential effects of an action more visible in context. In one solution, users can view their effective permissions as they change their privacy settings.[22]

Another major problem is that users encounter great difficulties in effectively configuring their privacy settings. To successfully use their settings, users must first locate them and understand their semantics. Furthermore, the settings need to be at a meaningful granularity to express the users' disclosure preferences.

The response from the access control community, informed by user modeling research, has been to develop privacy settings that are more expressive and closer to the users' mental models of OSNs. Many proposed access control models leverage users' "attributes," including relationships, roles, or other contextual information, 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.[23]

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, policymakers, and 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 companies' incentives to design systems that are comfortable for their customers.

Discussion

The surveillance and social policy 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 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. However, the issue is that the surveillance and social privacy approaches might 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 that 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 OSN privacy problem articulated?
- Which user activities and information in OSNs are in the scope of the privacy problem?
- What research methods should be used to approach OSN privacy problems?
- What types of tools or design principles should we use to mitigate the issues associated with OSN privacy problems and why?
- How should these tools and design principles be evaluated?

We believe that a more thorough analysis of the different approaches' answers will pave the way to a possible integration and a more comprehensive approach to addressing users' privacy problems in OSNs. In this article, we focus on the first three questions. The latter three are predicated on the answers to these questions and are important questions of inquiry for future research.

Who Has the Authority to Articulate the Privacy Problem?

In PETs research, security experts articulate what constitutes a privacy problem; in HCI, it's the average OSN user who does so.

With PETs, the emphasis is on the privacy risks that might arise when adversaries exploit technical vulnerabilities: this puts the security experts in the driver's seat, with 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, researchers bracket out the need to consider social and political analyses of surveillance practices. This introduces the risk of overrelying on technocentric assumptions about how surveillance functions and which strategies are the most appropriate to counter it. Moreover, the focus on improving security guarantees and designing tools that behave predictably in every context inevitably downplays the importance of the social context and users' talents in subverting technical boundaries in unexpected ways. It also deemphasizes the importance of considering the difficulties users might face in integrating these tools in their everyday lives.

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 might differ from the designers' use cases. However, the focus on contextual practices inevitably results in small, intensive studies. Surveys have a greater reach, but like small studies, they focus on individual users' perceptions and concerns. Hence, such studies don't provide much insight into collective privacy practices of established OSN communities, for example, specific interest groups.

Moreover, although user studies explore the correlations between demographics and privacy concerns, they rarely consider surveillance practices and how they might shape the privacy problem for specific populations. For example, underprivileged groups that are subject to greater surveillance might have other (social) privacy problems that are predicated on constraints with respect to the OSNs they might have access to, how they access these OSNs (for example, through shared devices or public libraries), and the quality of privacy features in different OSNs for negotiating social privacy. This might require examining other demographic criteria in user studies, for example, immigrants or lower-income communities. Furthermore, most of the studies are done with users in North America and Europe; few consider the needs of users elsewhere. For example, it's unclear if a study focused on activists or users in contexts with limited information and communications technology access would reveal the same privacy concerns. However, conducting such studies remains extremely challenging—researchers don't always have easy access to these communities, and the studies' design would need to account for their specific sociopolitical context.

Finally, as OSNs become integrated in 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 consider the values and ideologies embedded in a particular OSN design or to imagine radical design alternatives might overwhelm participants and fail to provide results. To address this limitation, we might need to introduce other methods, for example, workshops in which experts explore designs together with users.

How Is the Privacy Problem Articulated?

Whoever has the authority to articulate the privacy problems inevitably determines how these problems are defined. In both approaches, this entity 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 can't 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 risks might affect certain parts of the OSN population. For example, users deemed as not fitting societal norms might be discriminated against 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 might result in an erosion of basic rights and freedoms.

Often, even experts struggle to articulate how the abstract risks associated with OSN surveillance might materialize into actual harm. In practice, establishing the link between personal data disclosures and their ultimate consequences might even be impossible

because of the complexity and opacity of the data holders' decision-making processes. These processes involve multiple entities and data sources 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 haven't disclosed this information. The inferred preferences might or might not be correct, and we don't know if OSN providers employ such inference mechanisms. If they do, we don't 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 requires access to algorithms and management decisions that aren't typically available for scrutiny by either users or independent experts. OSN providers' opacity poses an enormous challenge to both PETs research and social privacy.

PETs designers can only guess which data is collected and how it could be exploited to the users' disadvantage. Without information on actual OSN surveillance practices, it's hard to establish the adversaries' capabilities and objectives or the accuracy of the risk analysis. In such cases, the researchers prefer to study worst-case scenarios. Although this is technically sensible, it might 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 might empower users to find their positions on matters that don't seem to directly impact them. How to conduct studies that surface the user perspective on abstract risks and harms remains an open question.

What Is in the Scope of the Privacy Problem?

The surveillance and social privacy approaches differ 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, that is, intended disclosures and interactions. Consequently, user studies are more likely to raise concerns with respect to explicitly shared data (for example, posts and pictures) than implicitly generated data (for example, behavioral data). In contrast, PETs research mainly focuses on guaranteeing concealment of information to unauthorized parties. Here, any data—explicit or implicit—that can be exploited to learn something about users is of concern.

Shedding light on users' perception of implicit data might benefit both approaches. Studies showing how aware users are of implicitly generated data might help them better understand their privacy practices. The results of such studies might also provide indicators for how we can more effectively deploy PETs. If users aren't aware of implicit data, we might want to explore designs that make implicit data more visible to them.

The content of the data shared by the user with trusted entities is out of PETs' scope. Researchers consider only the disclosure of data with respect to the adversary; PETs offer no protection to data disclosures made at the user's discretion, for example, to trusted friends. Furthermore, the data's semantics are also out of PETs' scope. However, social privacy studies reveal that users' privacy concerns include the semantics of intentional data disclosures toward 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 users' ability to express themselves shielded from pressure by peers and authorities. PETs can conceal who is speaking and what's being said in a content-agnostic manner. On the other hand, in social privacy approaches, self-censorship is explored as a strategy. For example, some solutions aim to avoid regrettable disclosures by cautioning users when they're 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 the norms underlying privacy nudges—for example, who decides what constitutes sensitive content?

Finally, users might benefit from being able to question norms asserted through design. There are situations in which OSN providers make certain actions invisible to avoid conflict; for example, in Facebook, users aren't 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's missing in social privacy research and that's 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?

By juxtaposing their differences, we identified how the surveillance and social privacy researchers ask complementary questions. We also made some first attempts to identify questions we might want to ask in a world in which 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 might 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 IWT SBO SPION, FWO G.0360.11N, FWO G.0686.11N, and GOA TENSE (GOA/11/007) projects.

References

1. "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network," Federal Trade Commission, 30 Mar. 2011; www.ftc.gov/opa/2011/03/google.shtm.
2. J. Grimmelmann, "Saving Facebook," *Iowa Law Rev.*, vol. 94, 2009, pp. 1137–1206.
3. K. Raynes-Goldie, "Privacy in the Age of Facebook: Discourse, Architecture, Consequences," PhD thesis, Curtin Univ., 2012.
4. N. Andrade, A. Martin, and S. Monteleone, "'All the Better to See You with, My Dear': Facial Recognition and Privacy in Online Social Networks," *IEEE Security & Privacy*, vol. 11, no. 3, 2013, pp. 21–28.
5. D.K. Mulligan and J. King, "Bridging the Gap between Privacy and Design," *J. Constitutional Law*, vol. 14, no. 4, 2012, pp. 989–1034.
6. G. Greenwald, "Hillary Clinton and Internet Freedom," *Salon*, 9 Dec. 2011; www.salon.com/2011/12/09/hillary_clinton_and_internet_freedom.
7. E. Morozov, "Facebook and Twitter Are Just Places Revolutionaries Go," *The Guardian*, 11 Mar. 2011; www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians.
8. M. Aouragh and A. Alexander, "The Egyptian Experience: Sense and Nonsense of the Internet Revolutions," *Int'l J. Comm.*, vol. 5, 2011, pp. 1344–1358.
9. I. Van Der Ploeg, *Keys to Privacy: Translations of "the Privacy Problem" in Information Technologies*, Maastricht: Shaker, 2005, pp. 15–36.
10. K.D. Haggerty and R.V. Ericson, "The Surveillant Assemblage," *British J. Sociology*, vol. 51, no. 4, 2000, pp. 605–622.
11. L. Palen and P. Dourish, "Unpacking 'Privacy' for a Networked World," *Proc. Int'l Conf. Human Factors in Computing Systems* (CHI 03), ACM, 2003, pp. 129–136.
12. F. Beato, M. Kohlweiss, and K. Wouters, "Scramble! Your Social Network Data," *Privacy Enhancing Technologies*, LNCS 6794, Springer, 2011, pp. 211–225.
13. E. de Cristofaro et al., "Hummingbird: Privacy at the Time of Twitter," *IEEE Symp. Security and Privacy*, IEEE CS, 2012, pp. 285–299.
14. J. Anderson et al., "Privacy-Enabling Social Networking over Untrusted Networks," *ACM Workshop Online Social Networks* (WOSN 09), ACM, 2009, pp. 1–6.
15. J. Anderson and F. Stajano, "Must Social Networking Conflict with Privacy?," *IEEE Security & Privacy*, vol. 11, no. 3, 2013, pp. 51–60.
16. A. Cutillo, R. Molva, and T. Strufe, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust," *Communications Magazine*, vol. 47, no. 12, 2009, pp. 94–101.
17. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," *Usenix Security Symp.*, Usenix, 2004, pp. 303–320.
18. F. Stutzman and W. Hartzog, "Boundary Regulation in Social Media," *Proc. Conf. Computer Supported Cooperative Work* (CSCW 12), ACM, 2012, pp. 769–778.
19. A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy*, vol. 3, no. 1, 2005, pp. 26–33.
20. B. Berendt, O. Günther, and S. Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior," *Comm. ACM*, vol. 48, no. 4, 2005, pp. 101–106.
21. Y. Wang et al., "I Regretted the Minute I Pressed Share: A Qualitative Study of Regrets on Facebook," *Proc. 7th Symp. Usable Privacy and Security* (SOUPS 11), ACM, 2011, art. 10.
22. H.R. Lipford et al., "Visual vs. Compact: A Comparison of Privacy Policy Interfaces," *Proc. 28th Int'l Conf. Human Factors in Computing Systems* (CHI 10), ACM, 2010, pp. 1111–1114.
23. R. Sayaf and D. Clarke, "Access Control Models for Online Social Networks," *Social Network Engineering for Secure Web Data and Services*, IGI Global, 2012.

Seda Gürses is a postdoctoral researcher at COSIC (Computer Security and Industrial Cryptography) in the KU Leuven's Department of Electrical Engineering. Her research interests are topics at the crossing of privacy technologies, surveillance studies, and requirements engineering. Gürses received a PhD in computer science from the KU Leuven. Contact her at seda.guerses@esat.kuleuven.be.

Claudia Diaz is an assistant professor in privacy technologies at COSIC in the KU Leuven's Department of Electrical Engineering. Her research focuses on privacy-enhancing technologies; she has published on topics including anonymous communications, anonymity metrics, steganographic file systems, location privacy, privacy in social networks, traffic analysis, and privacy by design. Diaz received a PhD in engineering from the KU Leuven. Contact her at claudia.diaz@esat.kuleuven.be.