Analyzing Privacy in Social Networks - An Interdisciplinary Approach

Michael Netter, Sebastian Herbst, Günther Pernul
Department of Information Systems
University of Regensburg
Regensburg, Germany
firstname.lastname@wiwi.uni-regensburg.de

***Abstract*—The rise of the social web has traditionally been accompanied by privacy concerns. Research on social web privacy has been conducted from various directions including law, social and computer sciences contributing to the body of literature. In this paper, we argue for an interdisciplinary approach to capture the multidimensional concept of privacy. For this purpose, we propose a three-layered framework to systematically analyze the privacy impact of various research directions. Subsequently, we conduct an interdisciplinary literature analysis, highlighting areas for improvement as well dependencies between different research directions.**

I. Introduction

Over the last decade, the evolution of the WWW led to a significant growth of Online Social Networks (OSN) and is receiving much attention in research. While Social Networks have always been an important part of daily life, the advent of Web 2.0 and its easy-to-use services increasingly shift social life to their online counterparts. OSNs provide an infrastructure for communication, information and self-expression as well as for building and maintaining relationships with other users.

The rise of relevance and quantity of social web services has been accompanied by privacy concerns. One the one hand, these worries arise due to the prevalent oligopolistic social web landscape with only few service providers possessing large databases with millions of user profiles. On the other hand, privacy concerns target the challenges of presenting different facets of the self to different audiences and to keep those views consistent. While this bears resemblance to managing different appearances of the self in the real world, the inherent properties of mediated OSN communication (e.g. permanency and searchability of personal information) put privacy at risk. Although privacy controls are in place to currently restrict access to personal data, users seem to be shortsighted concerning future issues of current behavior [45].

Both aforementioned areas of privacy have been intensively tackled by research from various directions such as law, social and computer sciences. Yet, the ambiguous nature of privacy and multiple definitions available impede a consistent view on the concept. Concerning this, Robert C. Post notes that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[37]

In this paper, we stress the need for integrating the insights from diverse islands of research on social web privacy. We contribute to this field by providing a framework to decompose social web privacy and systematically analyze the impact of different research directions. Subsequently, we apply the framework to the body of research. Our results highlight areas for improvement as well as dependencies between different research directions emphasizing the necessity to foster interdisciplinary research on social web privacy.

The remainder of this paper is structured as follows: In the next Section, we give an overview of related work. In Section III, we decompose social web privacy and transfer its components into a framework for analyzing the concept from different research directions. We apply our framework on the existing body of research, differentiating between privacy issues related to OSN users and to OSN service providers in Section IV and Section V. Finally, in Section VI, we summarize our findings and highlight areas for future work.

II. Related Work

In this Section existing approaches that aim to integrate several research directions to create a holistic view on privacy are presented. Note that approaches for particular aspects of privacy are discussed in our detailed impact analysis of the various privacy perspectives in Section IV and Section V.

Spiekermann and Cranor provide a framework to build privacy-friendly systems [42]. The authors distinguish between privacy-by-policy and privacy-by-architecture. While the former is a legally-driven approach that focuses on notifying the user and obtaining his consent prior to processing personal data, the latter is a technically-driven approach to minimize the collection of personal data without limiting functionality. Their approach however does not consider the social perspective of privacy and focuses on privacy in general while this work is on social web privacy. The importance of social web privacy is acknowledged by the European Union, promoting several research projects. PADGETS aims at an interdisciplinary approach to strengthen users' privacy while harnessing social network data for policy making. Similarly, the European research project PrimeLife has developed a framework to analyze privacy issues related to other OSN users [39]. Project results show that privacy issues arise, when legal or social norms are disregarded or technical safeguards are

	Privacy issues related to	
	OSN Users	**OSN Service Providers**
Legal	International Standards (OECD Privacy Principles, EU Data Protection Framework), National Laws	International Standards (OECD Privacy Principles, EU Data Protection Framework), National Laws, Privacy Policies
Technical	Cryptography And Steganography, Privacy Agents, Fine-grained Access Control Models, Visualization Of Personal Data	Cryptography And Steganography, Privacy Agents
Social	Peer-group Pressure, Trust Relationships, Tie Strength, Privacy Awareness	Privacy Awareness, Pressure Of The Media

TABLE I
PROPOSED THREE-LAYERED FRAMEWORK FOR ANALYZING SOCIAL WEB PRIVACY

circumvented. Depending on the owner's initial categorization of personal data (private, semi-public, public), the presented framework allows estimating potential privacy risks. Unlike our approach, this work does not take privacy threats stemming from OSN service providers into account, but solely focuses on user-related privacy issues. PRESCIENT, another EU funded project conducted an in-depth study of privacy conceptualizations [25]. It takes a legal, social, economic and ethical perspective on privacy, highlighting similarities and interdependencies. This project results provide useful insights to increase the general understanding of the concept of privacy, however the analyses do not follow a structured approach as shown in this paper.

III. PROPOSED THREE-LAYERED FRAMEWORK

In this Section, an overview of our proposed framework is provided. The framework aims at providing a general-purpose structuring of social web privacy research domains. Subsequently, the concept of privacy is broken up into a set of characteristics that are subsequently used to conduct our impact analysis in Section IV and Section V.

A. Overview

In their conceptualization of privacy in the year 1890 as "the right to be let alone", Warren and Brandeis were one of the first to recognize the multidimensionality of the privacy concept [48]. Until then, privacy threats were primarily related to a potential physical harm [40]. The rise of the information age led to a large number of privacy conceptualizations from a variety of directions such as social sciences, law, architecture, urban design, health sciences, and computer and information sciences. In their work to structure the concept of privacy, Patil and Kobsa introduce three main perspectives to describe and analyze privacy [35]:

Legal: Focuses on laws and policies aiming to protect the individual from corporations, governments and other individuals. For instance, the European Data Protection Framework promotes informational self-determination emphasizing an individual's rights to control the collection and use of personal data [18].

Technical: Aims to translate norms and regulations into technical specifications. The Platform for Privacy Preferences Project (P3P) is an example for enhancing the individual's ability to control information disclosure by technical means [13].

Social: Concentrates on managing social relationships and the boundaries between private and public life. For instance, Nissenbaum describes privacy as contextual integrity, arguing that personal information is published within a well-defined social context [33]. Privacy is breached if personal information is available outside its intended context.

For this work, we adapt this three-layered view and extend it to cover privacy risks of online social networks. Typically, two distinct areas of research can be observed [49] [6]:

OSN Service Providers: Research in this direction includes means to legally bind service providers to comply with current legislation, to increase end-user trust in service providers and to provide technical safeguards, e.g. by cryptographic or steganographic means [24].

OSN Users: Research aims to recreate the different social contexts of the real world, e.g. by supporting an individual to segment its social streams for specific audiences and providing means to have different digital identities [47].

The two aforementioned research directions are combined with the three perspectives on privacy (legal, technical, and social) resulting in our proposed framework. The framework is shown in Table I, with the cells containing concepts that become relevant for the respective dimension. Note that the three dimensions are not mutually exclusive but interdependent. Subsequently, in Section III-B the two research directions (OSN Service Providers and OSN Users) are further decomposed into a set of privacy characteristics derived from literature review. These privacy characteristics are not exhaustive but rather aim at providing a solid foundation for analyzing the impact of the three perspectives on privacy. In the following, these characteristics are described in detail.

B. Characteristics to analyze social web privacy

Data Sovereignty: Describes to what extend an individual is able to control the processing of its personal data [4]. Personal data in OSN it typically available in a structured manner and can easily be copied, linked, aggregated, and

transferred [39]. Consequently, it is difficult for an OSN user to control the flow of personal information and thus putting privacy at risk. The problem increases as OSN typically lack the spatial, social, and temporal boundaries of the real world which limit the flow of personal information by default [9].

Data Transience: Revolves around the loss of personal information over time which can be considered typical characteristic of real-world communication [39]. In contrast, the mediated communication of OSNs results in a permanent storage of personal information. Mayer-Schönberger notes that "[s]ince the beginning of time, for us humans, forgetting has been the norm and remembering the exception. [..] Today, with the help of widespread technology, forgetting has become the exception, and remembering the default." [31] In addition, this permanency of personal information poses a great challenge to privacy, since we are no longer free in constructing our identities because contradictory information may be available online [41].

Protection against profiling: Subsumes an individual's ability to prevent an adversary from collecting, aggregating and linking personal data in order to create a digital dossier [23]. Such profiling threats are increased if secondary data such as location (e.g. stemming from mobile phones) and connection logs are linked with existing OSN profiles [27]. The current landscape of social web service providers with their targeted advertising-centered business models and large identity silos additionally adds to this threat.

Audience Segregation: Originally developed by Goffman [21], it states that each individual performs multiple and possibly conflicting roles in everyday life, and it needs to segregate the audiences for each role, in a way that people from one audience cannot witness a role performance, that is intended for another audience and thereby keep a consistent self-image and maintain privacy [46]. In current OSNs, contacts are typically classified as "friends", making it difficult to selectively share personal information with a specific group of people. As a result, privacy is threatened because a large audience might have access to personal information.

Privacy Awareness: Encompasses attention, perception, and cognition of which personal information others have received and how this information is or may be processed [38]. An individual's awareness for privacy risks is a prerequisite for privacy-preserving behavior.

Transparency: With regards to OSN service providers, transparency describes the user's possibility to inform oneself of processing and dissemination practices [10]. Taking a social point of view, transparency implies an individual's possibility to recognize contextual boundaries, which is important to contextual integrity [33].

Enforcement: Comprises an individual's means to bring his privacy preferences into force. With regard to OSN service providers and OSN users, it describes the extent to which an individual can control adherence to privacy settings and limitations [11].

Table II provides a summary of the presented characteristics of privacy. Most properties apply to privacy issues related to social web users as well as to service providers, while audience segregation only applies to the former and protection against profiling only applies to the latter.

	Relevant for privacy issues related to	
	OSN Users	OSN Service Providers
Data Sovereignty	Yes	Yes
Data Transience	Yes	Yes
Protection against profiling	No	Yes
Audience Segregation	Yes	No
Privacy Awareness	Yes	Yes
Transparency	Yes	Yes
Enforcement	Yes	Yes

TABLE II
PRIVACY CHARACTERISTICS OVERVIEW

C. Classification scheme

For the classification, we facilitate a four-step ordinal scale (none, minor, medium, and major impact) for rating the impact of the previously defined dimensions (legal, technical and social) in the next two Sections. No impact (none) indicates that a certain dimension does not contribute to enhancing privacy. A minor impact implies that it only provides supportive means, whereas a major impact expresses that it is a key driver for strengthening privacy. A medium impact indicates that a certain dimension has theoretical relevance for strengthening privacy but practical limitations reducing their applicability. Note that the application of an interval scale (quantitative) is not feasible throughout such a qualitative analysis, which aims at highlighting impacts of and dependencies between different research directions.

In the following, the analysis of each privacy characteristic is based on a structured scheme: At first, legal aspects are analyzed highlighting their impact on both privacy issues related to OSN users as well as OSN service providers. Secondly, the impacts of existing technical approaches for enhancing social web privacy are discussed. Finally, the implications of social norms on strengthening privacy in the given scenario are examined.

IV. PRIVACY ISSUES RELATED TO SOCIAL WEB USERS

In this Section we conduct an impact analysis of privacy issues related to OSN users. The results are summarized in Section IV-G.

A. Data Sovereignty

From a legal point of view, laws and policies applicable to govern the exchange and flow of personal information between people are typically not available. Thus the legal dimension does not contribute to data sovereignty with regard to other OSN users (no impact).

In addition to the legal dimension of data sovereignty, several technical approaches have been proposed to support a context-sensitive disclosure of personal data strengthening data sovereignty. For instance, access control models that enable the

user to map their real world's trust relationships to OSNs have been introduced [12]. Such technical approaches in general aim at recreating the real world's social norms. Thus, they can be considered a useful means to strengthen data sovereignty, however, their overall impact is minor due to their limited supportive character.

From a social point of view, data sovereignty is threatened if personal information is taken out of its intended context. Tagging people on pictures – a common feature of OSNs – is a typical example of losing control of personal data flows. Gross and Acquisti argue that social norms can strengthen data sovereignty if the fine-grained social relations of the real world can be transferred to OSNs as these foster reliability and predictability of other user's behavior [23]. However, adherence to social norms highly depends on the trust relationship between two users, which are commonly divided in weak ties and strong ties [17]. Strong ties typically reflect relations with well-known acquaintances and an abuse of confidence is likely to have an negative impact on their real-world relationship [17]. In contrast, studies indicate that users tend to have increasingly weak ties in OSNs, lacking fine-grained social relations [8] [23]. Individuals are commonly viewed as "contacts" or even called "friends". Examining the impact on privacy issues related to other OSN users, unauthorized disclosure can primarily be regarded a social problem that relies on strong ties to be effective. As a consequence, the overall impact of social aspects is medium, due to the aforementioned prevalent weak ties of current OSNs.

B. Data Transience

Digitally mediated communication differs from real world communication as the former adds persistence, searchability, replicability, and scalability by default [9]. However, other OSN users typically cannot be legally forced to delete voluntarily shared personal information after a given period of time. As a consequence, there is no legal impact on data transience regarding other users.

From a technical perspective, putting an expiry date on personal data is difficult as digital information that is eventually available can easily be copied. While approaches to technical data transience exist, successful attacks as demonstrated in [19] substantiate their minor impact.

From a social point of view, the permanency of personal information in OSNs poses major challenges. According to Gross and Acquisti, OSN users are typically unaware of the existing data storage periods [23]. Consequently, we deduce a lack of social norms regarding data persistence and conclude that there is no impact stemming from social aspects.

C. Audience Segregation

Managing the presentation of the self to different audiences is a social challenge which is not governed by legal regulations (no impact).

From a technical perspective, audience segregation is partially implemented in common OSNs (e.g. Facebook Groups[1] and Google Circles[2]). In addition, audience segregation is starting to gain attention in the research community. The prototypical OSN Clique[3], developed within the PrimeLife project, for instance, implements a fine-grained access control mechanism to present each audience with a different view on a user's identity [46]. Another approach presented in [32] automatically determines distinct audiences based on the user's relationships. In the current state, a medium impact of audience segregation on OSN user privacy can be deduced. However, the increasing research activities indicate a future growth of the importance of technical means.

Taking a social point of view, audience segregation is a useful concept to apply the theory of contextual integrity as outlined in Section III. Currently however, audience segregation is not well-supported in existing OSNs and thus users resort to behavioral strategies such as choosing appropriate communication channels (e.g. private messages) as well as to mental strategies (e.g. self-censorship) [29]. Studies show that managing different audiences is a burden to many users and rarely applied [15]. Following the results of the aforementioned studies, only a medium social impact of audience segregation to privacy can be inferred.

D. Privacy Awareness

Awareness is an important requirement of social web privacy that affects many of the characteristics presented in Section III. However, from a regulatory point of view, OSN user awareness cannot be legally enforced (no impact).

Technical aspects such as usable user interfaces influence the perceived privacy protection and the awareness of privacy risks [22]. However, similar to previous characteristics, technical means only have a supportive character to facilitate privacy awareness and point at potential privacy violations (minor impact).

Privacy awareness is primarily a social concept with a gap existing between theoretical and practical privacy awareness [10]. This is backed by further studies indicating that OSN users are frequently underestimating privacy risks and rarely use available privacy settings [2] [23]. According to Acquisti, immediate gratifications outweigh long-term privacy risk and lead to a myopic evaluation of privacy risks [1]. In summary, there is a medium social impact on the privacy protection from other users due to the discrepancy between theoretical and practical impact of privacy awareness.

E. Transparency

While bearing resemblance to privacy awareness, transparency aims at enhancing the user's understanding on the propagation of his personal data within an OSN to better protect this data from unauthorized access. From a legal perspective, an individual has little means to force other users to make their proliferation of others' personal data transparent as typically no respective regulations exist.

[1] http://www.facebook.com

[2] https://plus.google.com

[3] http://clique.primelife.eu/

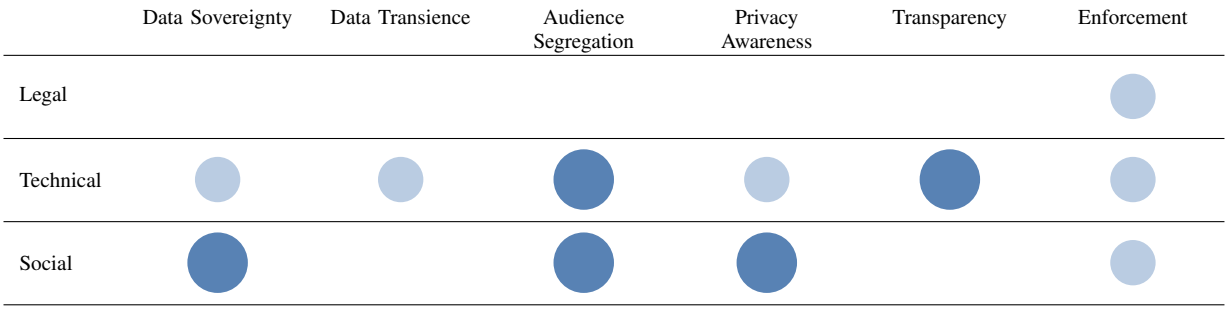

TABLE III
SUMMARY OF USER RELATED IMPACT ANALYSIS (IMPACT: ■ DARK-BLUE≙MAJOR, ■ MID-BLUE≙MEDIUM, ■ LIGHT-BLUE≙MINOR)

Taking a technical point of view, transparency-enhancing approaches focusing on logging and retrospective analysis of personal data disclosures have been proposed [28]. Additionally, it has been shown that weak ties and loose sharing preferences (e.g. friend-of-a-friend) may lead to a large personal network and non-transparent personal data spreading [23]. Technical approaches to visually improve personal network transparency have been proposed, underlining that transparency highly depends on the OSN service provider and provided application programming interfaces (APIs) [44]. Following this argumentation, the technical impact has to be regarded medium as many transparency mechanisms rely on APIs to be provided by OSN service providers.

Similar to the legal dimension, the spreading of personal information by other OSN users is typically not governed by social norms, leading to no social impact on transparency.

F. Enforcement

From a legal point of view, enforcement of law is an inherent property of any legal system. In the context of social web privacy, an individual can seek for an injunction if reputation-damaging information is published. However, legal means are not universally applicable to the social web. Following the European Court of Justice, legal protection requires personal information to be restricted to close friends and family members to be applicable [16]. In addition, legal means only allow suing others after a privacy breach leading to a minor overall impact of legal enforcement on the privacy protection against other users.

Additionally, technical means may have a positive impact on the enforcement of legal steps. However, current OSNs greatly differ in providing technical means to move in on such aspects (e.g. cyber-bulling) [7]. Thus, these means can be considered to only have a supportive function with a minor impact.

Investigating privacy enforcement from a social perspective, tie strength plays an important role. In some cases, a specific group of an individual's OSN (e.g. family members) may have established social norms that allow each member to employ peer-group pressure to enforce his privacy interests [20]. Following the argumentation of [23] that relationships in OSNs often consist of weak ties the social impact on the enforcement of peer-pressure can be considered minor.

G. Summary

Table III summarizes the results of our impact analysis using the proposed framework. This Section has underlined that privacy protection from other social web users is predominately covered by social norms. This corresponds to the real world, where users mainly rely on selective sharing of personal data and highly differentiated relationships to ensure privacy. The mediated nature of OSNs (e.g. permanent storage and searchability of personal data) adds a new layer of complexity. This influences privacy as the informational environment of OSNs is counterintuitive to the norms of personal data distribution of the real world. This often leads to a violation of contextual integrity [36]. Table III points out that technical approaches to privacy can be seen as supportive means to translate social norms to the OSNs with a potentially increasing importance in the future. On the contrary, legal measures play a minor role and are a last resort to retroactively punish privacy violations. These observations corresponds to those of Strahilevitz, stating that law does little to shape people's actual expectations of privacy [43].

V. PRIVACY ISSUES RELATED TO SERVICE PROVIDERS

Following the analysis of privacy issues related to social web users, this Section investigates the impact of service provider related privacy issues. Subsequently, the results are summarized and integrated into our framework.

A. Data sovereignty

To ensure data sovereignty, legal norms have been enacted to control the exploitation of personal data by OSN service providers [16]. For instance, according to the German Teleservices Act and the Federal Data Protection Act, service providers require the user's explicit consent to use personal data for advertising purposes [16]. Furthermore, legal requirements for OSN service providers comprise the secure storage of personal data and exclusion of search indexes by default. Consequently, legal aspects have a high impact on strengthening an individual's data sovereignty.

From a technical point of view, several approaches to facilitate data sovereignty have been proposed (e.g. [5], [24]). These approaches rely on cryptographic and steganographic means to effectively protect an individual's personal data from

service provider access. Although they can easily be integrated into current OSN, they commonly infringe the service provider's general terms and conditions as their business model typically relies on free access to personal data for advertising purposes [39]. Hence, despite the theoretical effectiveness of the aforementioned approaches, the practical difficulties lead to a only medium technical impact on data sovereignty.

Commonly, OSN users do not have any social relationship with OSN service providers. As a consequence, an individual cannot rely on social means to ensure the service provider's adherence to data sovereignty. Thus there is no impact stemming from this dimension.

B. Data Transience

Similar to data sovereignty, data transience is well-covered by legal norms and regulations to be fulfilled by OSN service providers. Providers are required to entitle a user to delete all personal data stored in a OSN profile and to cancel his membership [16]. Similarly, the European Data Protection Framework requires personal data to be removed, if the purpose for which the data was collected ceases to exist [18]. This puts the user in a strong position and leads to a high legal impact on data transience.

Approaches like [19] can be applied to technically enforce data transience in respect to OSN service providers. However, their impact in general can be considered as minor as most of the OSN service providers prohibit any tools that put access restrictions on personal data in their general terms and conditions.

Similar to the previous argumentation dealing with data sovereignty (see Section V-A), the missing social relationship between OSN users and OSN service providers leads to no social impact on enforcing data transience.

C. Protection against Profiling

Privacy threats stemming from OSN service providers have been recognized by the OECD privacy principles [34] as well as the EU Data Protection Framework [18]. Therein, data minimization is one of the key principles to prevent service providers from linking personal information and thus from building digital dossiers. However, several of the social web's underlying principles counteract data minimization. For instance, the business models of OSN service providers mostly rely on personal data being used for advertising purposes. As a consequence, several personal attributes are mandatory for registration. Studies indicate that only 3 out of 29 OSNs allow for a fully pseudonymous registration [7]. This leads to the conclusion that, despite existing legal regulations to protect the user against profiling, the legal impact in practice can be considered as minor.

Technically, approaches presented in Section V-A can be applied to prevent profiling. Other research directions include the application of user-centric identity management systems on OSNs to strengthen the user's control and to prevent service provider- and third party access without prior approval. Maliki and Seigneur, for instance focus on the concept of Identity 2.0 and respective implementations [30]. Concluding, technical approaches in practice only have a minor impact on the protection against profiling, as the general terms and conditions of OSNs commonly prevent their application.

Again, due to the typically missing strong ties between OSN users, social norms are not applicable for protecting against profiling (no impact).

D. Privacy Awareness

Similar to user-related privacy threats (see Section IV-D), awareness is primarily influenced from a social perspective, while legal and technical means do not contribute at all.

Studies reveal that users of Facebook, for instance, put more trust in the service provider than in average Facebook users [2]. They further show that 56 percent believe that Facebook does not share personal information with third parties and 70 percent believe that Facebook does not combine information about them collected from other sources. Less than one out of four users claims to have read Facebook's privacy policy. While privacy risks tend to remain invisible to the average user [14], awareness raises, if privacy-invading features are introduced such as Facebook's News Feed [26]. Note that a high awareness generally is seen as a major obstacle in generating revenue by OSN service providers [49]. This leads to the conclusion that while awareness increases in exceptional situations, OSN users become accustomed to privacy threats stemming from service providers and thus leading to a medium social impact on privacy awareness.

E. Transparency

The primary source of information to assess the legal impact on transparency is the service provider's privacy policy. For this purpose, Bonneau and Preibusch extensively analyzed the privacy policies of 45 OSN providers [7]. As a result, flaws in almost all privacy policies, ranging from bad technical accessibility (e.g. by requiring JavaScript) to extensive use of legal jargon which is far too difficult for ordinary users to understand have been identified. Further issues include a missing specification of applicable national data protection laws and the nation in which the data is stored and processed. The results show that there is no significant correlation between a network's privacy score and actually privacy practices.

A similar study on service provider transparency reveals that users are often unable to determine the amount of required personal data prior to the registration [10]. It additionally shows that even upon request by e-mail, service providers often do not provide adequate support to increase transparency of their data handling practices. Consequently, despite the existence of privacy policies as valuable legal means to foster transparency, there is only a medium legal impact due to the aforementioned restrictions in their practical implementation.

Besides legal means, several technical approaches to service provider transparency have been developed with P3P being a prominent example [13]. P3P requires the service providers to publish a machine-readable privacy policy that subsequently can be matched with the user's predefined privacy preferences.

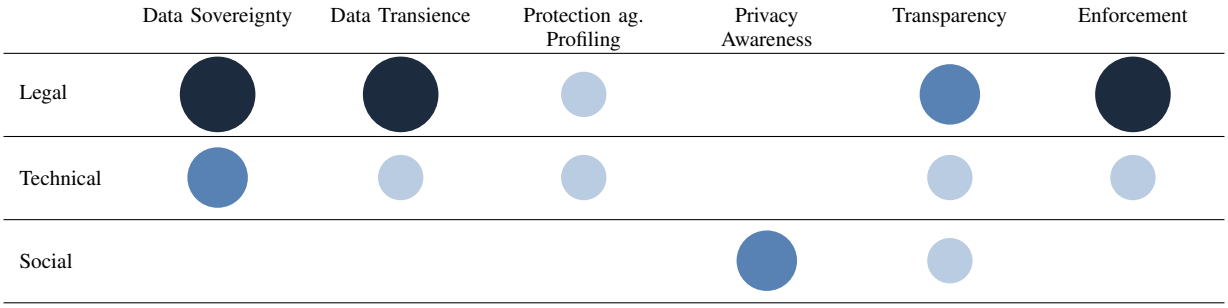

TABLE IV
SUMMARY OF SERVICE PROVIDER RELATED IMPACT ANALYSIS (IMPACT: ■ DARK-BLUE≙MAJOR, ■ MID-BLUE≙MEDIUM, ■ LIGHT-BLUE≙MINOR)

However, most OSN service providers do not provide a machine-readable version of their privacy policy and thereby making P3P inapplicable [7]. Additionally, the task of defining privacy preferences can hardly be executed by non-technical users [3]. Taking these shortcomings into account, there is only a low impact of technical means to facilitate transparency.

Approaching transparency from a social perspective, media coverage plays an important role in communicating personal data handling practices of social web service providers [7]. Yet, they typically do not provide a profound analysis of privacy problems but focus on partial aspects of privacy. The minor impact of mass media on transparency is also backed by the lack of privacy awareness (see Section V-D). This leads to a minor overall impact of social means to foster transparency.

F. Enforcement

The inherent enforceability of legal measures (see Section IV-F) also applies to OSN service providers and is also reflected in the dominance of legal impact in the previous Sections. OSN service providers typically employ a privacy-by-policy approach (e.g. as defined in [42]), notifying and obtaining the user's consent to its privacy policy prior to registration and thereby strengthening the legal impact to enforce privacy interests (high impact).

Regarding the technical perspective, several means for enforcing OSN user's privacy preferences are available (see Section V-A and Section V-B). However, their overall practical impact is minor, taking into consideration that these tools are often prohibited by the service provider's general terms and conditions.

While social norms have a significant impact on enforcing privacy interests towards other users (see Section IV-F) there is typically no social relationship between a social web service provider and its users. As a consequence, power structures of social groups do not apply. In addition, the impact of mass media coverage is a limited tool to put pressure on service providers as already outlined in Section V-E. Thus, privacy interests towards service providers cannot be socially enforced (no impact).

G. Summary

Table IV sums up the results of our analysis of privacy issues related to OSN service providers. Two major conclusions can be derived: Firstly, a shift of impact from the social to the legal dimension compared to Section IV can be seen. The results secondly show an in general increased impact of all dimensions compared to Section IV-G. Particularly the major legal impact is noteworthy showing that legislators realize the unequal distribution of power and consequently try to strengthen the position of OSN users. In contrary, the minor impact of social norms can be explained by the diffusion of responsibility. As service providers are typically not embedded in an individual's social structure, social norms do not apply. Similar to the results of Section IV-G, technical tools can be seen as supportive means while their impact is often limited. Finally, the limited means of all three dimensions to protect an individual against profiling are noteworthy, emphasizing the service providers' efforts to protect their business model.

VI. CONCLUSIONS AND FUTURE WORK

The rising popularity of online social networks poses many challenges in the field of privacy. Unlike in the real world, where personal information is ephemeral, in the online-world, this information is almost infinitely available. This poses great challenges for managing identities online and context-sensitive sharing of personal information with other users. In addition, the prevalent oligopolistic social web landscape threatens privacy as it fosters the growth of identity silos.

We have argued for an interdisciplinary approach to tackle the aforementioned privacy risks. Consequently, as the main contribution of this paper, a framework to systematically analyze social web privacy issues from a legal, technical and social perspective has been proposed. Furthermore, the impact of those three different perspectives on privacy among OSN users themselves and between OSN users and service providers has been highlighted based on a thorough literature review. The results underline our initial assumption that the challenges of social web privacy cannot be tackled from a single direction but rather have to be addressed by a comprehensive interdisciplinary approach.

This leads to a variety of research directions for future work. For instance, the role of technology in pursuing social privacy violations has to be investigated in detail. Additionally we aim at overcoming the limitations of subjective qualitative characterization of privacy impacts by conducting a quantitative

study investigating social web privacy based on the framework presented in this paper. This could lead to further convergence of research activities.

ACKNOWLEDGMENTS

We would like to thank Ludwig Fuchs for his helpful remarks and valuable suggestions to improve this work. The research leading to these results is partly funded by the European Union within the PADGETS project under grant agreement no. 248920. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the European Union.

REFERENCES

[1] A. Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce (EC '04)*, 2004.

[2] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, 2006.

[3] R. Agrawal. Why is p3p not a pet? In *Proceedings of the W3C Future of P3P Workshop*, 2002.

[4] E. Aïmeur, S. Gambs, and A. Ho. Towards a privacy-enhanced social networking site. In *Proceedings of the Fifth International Conference on Availability, Reliability and Security*, 2010.

[5] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: an online social network with user-defined privacy. In *Proceedings of the ACM SIGCOMM Conference on Data communication*. o, 2009.

[6] M. Beye, A. J. P. Jeckmans, Z. Erkin, P. H. Hartel, R. I. Lagendijk, and Q. Tang. Literature overview - privacy in online social networks. Technical Report TR-CTIT-10-36, Centre for Telematics and Information Technology, University of Twente, Enschede, October 2010.

[7] J. Bonneau and S. Preibusch. The Privacy Jungle: On the Market for Data Protection in Social Networks. In *Proceedings of the 8th Workshop on the Economics of Information Security*, 2009.

[8] D. Boyd. Friendster and publicly articulated social networking. In *CHI '04 extended abstracts on Human factors in computing systems*, 2004.

[9] D. Boyd. *Taken Out of Context: American Teen Sociality in Networked Publics*. PhD thesis, University of California, Berkeley, 2008.

[10] T. Burghardt, E. Buchmann, and K. Böhm. Why do privacy-enhancement mechanisms fail, after all? A survey of both, the user and the provider perspective. In *Proceedings of the Workshop W2Trust*, 2008.

[11] B. Carminati and E. Ferrari. Access control and privacy in web-based social networks. *International Journal of Web Information Systems*, 4(4), 2008.

[12] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security*, 13:1–38, November 2009.

[13] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. M. Reagle, M. Schunter, D. A. Stampley, and R. Wenning. The platform for privacy preferences 1.1 (p3p1.1) specification. NOTE-P3P11-20061113, 2006.

[14] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1):83–108, 2009.

[15] J. M. DiMicco and D. R. Millen. Identity management: multiple presentations of self in facebook. In *Proceedings of the 2007 international ACM conference on Supporting group work*, 2007.

[16] A. Dix. Daten- und Persönlichkeitsschutz im Web 2.0. In D. Klumpp, H. Kubicek, A. Roßnagel, and W. Schulz, editors, *Netzwelt - Wege, Werte, Wandel*, pages 195–210. Springer Berlin Heidelberg, 2010.

[17] J. Donath and D. Boyd. Public displays of connection. *BT Technology Journal*, 22:71–82, 2004.

[18] European Parliament. EU-Directive 95/46/EC. *Official Journal of the European Communities*, 1995.

[19] H. Federrath, K.-P. Fuchs, D. Herrmann, D. Maier, F. Scheuer, and K. Wagner. Grenzen des digitalen Radiergummis. *Datenschutz und Datensicherheit - DuD*, 35:403–407, 2011.

[20] D. C. Feldman. The development and Enforcement of Group Norms. *The Academy of Management Review*, 9(1):47–53, Jan. 1984.

[21] E. Goffman. *The Presentation of Self in Everyday Life*. Anchor, 1959.

[22] J. Grimmelmann. Saving Facebook. *NYLS Legal Studies Research Paper No. 08/09-7*, 2008.

[23] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 2005.

[24] S. Guha, K. Tang, and P. Francis. Noyb: privacy in online social networks. In *Proceedings of the 1st workshop on Online social networks*, 2008.

[25] S. Gutwirth, R. Gellert, R. Bellanova, M. Friedewald, P. Schütz, D. Wright, E. Mordini, and S. Venier. Deliverable d1: Legal, social, economic and ethical conceptualisations of privacy and data protection, March 2011.

[26] C. M. Hoadley, H. Xu, J. J. Lee, and M. B. Rosson. Privacy as information access and illusory control: The case of the facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, 9(1):50 – 60, 2010. Special Issue: Social Networks and Web 2.0.

[27] G. Hogben. Security issues and recommendations for online social networks. Technical report, ENISA, 2007.

[28] J. Kolter, M. Netter, and G. Pernul. Visualizing past personal data disclosures. In *Proceedings of the Fifth International Conference on Availability, Reliability and Security*, 2010.

[29] A. Lampinen, S. Tamminen, and A. Oulasvirta. All my people right here, right now: management of group co-presence on a social networking site. In *Proceedings of the ACM International Conference on Supporting Group Work*, 2009.

[30] T. E. Maliki and J.-M. Seigneur. Identity management. In J. Vacca, editor, *Computer And Information Security Handbook*. Morgan Kaufmann, 2009.

[31] V. Mayer-Schönberger. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, Oct. 2009.

[32] M. Netter, M. Riesner, and G. Pernul. Assisted Social Identity Management - Enhancing Privacy in the Social Web. In *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, 2011.

[33] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books, 2010.

[34] OECD. Guidelines on the protection of privacy and transborder flows of personal data., 1980.

[35] S. Patil and A. Kobsa. Privacy considerations in awareness systems: Designing with privacy in mind. In *Awareness Systems*. Springer London, 2009.

[36] C. Peterson. Losing Face: An Environmental Analysis of Privacy on Facebook. *SSRN eLibrary*, 2010.

[37] R. C. Post. Three concepts of privacy. *GEORGETOWN LAW JOURNAL*, 1:2087–2098, 2001.

[38] S. Pötzsch. Privacy awareness: A means to solve the privacy paradox? In *The Future of Identity in the Information Society*. Springer Boston, 2009.

[39] PrimeLife. D1.2.1 - Privacy Enabled Communities, 2010.

[40] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006*, 154:477, 2006.

[41] D. J. Solove. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale Univ Pr, Nov. 2008.

[42] S. Spiekermann and L. F. Cranor. Engineering privacy. *IEEE Trans. Softw. Eng.*, 35:67–82, January 2009.

[43] L. Strahilevitz. A Social Networks Theory of Privacy. *University of Chicago Law Review*, 72(3):919–988, Dec. 2005.

[44] G. Tscherteu and C. Langreiter. Explorative Netzwerkanalyse im Living Web. In *Social Semantic Web*. Springer Berlin Heidelberg, 2009.

[45] Z. Tufekci. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 11:544–564, 2008.

[46] B. van den Berg and R. Leenes. Audience Segregation in Social Network Sites. In *Proceedings of the 2nd International Conference on Social Computing*, 2010.

[47] B. van den Berg and R. Leenes. *Keeping Up Appearances: Audience Segregation in Social Network Sites*, chapter 10. Springer, 2011.

[48] S. D. Warren and L. D. Brandeis. The right to privacy. *Harward Law Review*, 4:193–220, 1890.

[49] M. Ziegele and O. Quiring. Privacy in Social Network Sites. In S. Trepte and L. Reinecke, editors, *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer, 2011.