Interdisciplinary Impact Analysis of Privacy in Social Networks

Michael Netter, Sebastian Herbst, and Günther Pernul

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

1 Introduction

Over the last decade, the evolution of the World Wide Web led to the significant growth of Online Social Networks (OSNs), which are receiving much attention in the research community. 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 increase in relevance and the quantity of social web services has been accompanied by privacy concerns. On one hand, these worries have arisen due to the prevalent oligopolistic social web landscape with only a few service providers possessing large databases with millions of user profiles. On the other hand, privacy concerns focus on the challenges of presenting different facets of the self to different audiences, and to keep those views consistent. While this bears a

M. Netter (✉) • S. Herbst • G. Pernul
Department of Information Systems, University of Regensburg, Regensburg D-93040, Germany
e-mail: michael.netter@wiwi.uni-regensburg.de; sebastian.herbst@wiwi.uni-regensburg.de; guenther.pernul@wiwi.uni-regensburg.de

Y. Altshuler et al. (eds.), *Security and Privacy in Social Networks*,
DOI 10.1007/978-1-4614-4139-7_2,

resemblance to managing different appearances of the self in the real world, the inherent properties of mediated OSN communication (e.g., the permanency and searchability of personal information) places privacy at risk. Although privacy controls are in place to currently restrict access to personal data, users seem to be shortsighted with respect to future aspects of current behavior [1].

Both aforementioned areas of privacy have been studied extensively by researchers through various viewpoints such as law, the social sciences, and computer science. However, the ambiguous nature of privacy and the multiple definitions available impede a consistent view of the concept. Robert C. Post notes that privacy "... 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." [2].

In this chapter, we stress the need to integrate insights from diverse areas of research on social web privacy. We contribute to this field by providing a framework with which to decompose social web privacy and systematically analyze the effects of different research directions. Subsequently, we applied the proposed 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 chapter is structured as follows. In Sect. 2, we give an overview of related work. In Sect. 3, 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 OSN service providers in Sects. 4 and 5, respectively. Finally, in Sect. 6, we summarize our findings and highlight areas for future work.

2 Related Work

In this section, we present existing approaches that aim to integrate several research directions in order to create a holistic view of privacy. Approaches to particular aspects of privacy are discussed in our detailed impact analysis of the various privacy perspectives in Sects. 4 and 5.

Spiekermann and Cranor provide a framework with which to build privacy-friendly systems [3]. They distinguish between privacy-by-policy and privacy-by-architecture. The former is a legally-driven approach that focuses on notifying the user and obtaining consent prior to processing personal data. The latter is a technically-driven approach to minimize the collection of personal data without limiting functionality. However, their approach does not consider the social perspective of privacy and focuses on privacy in general, whereas our work examines social web privacy. The importance of social web privacy is acknowledged by the European Union, which is promoting several related research projects. For

example, PADGETS[1] uses an interdisciplinary approach to strengthen users' privacy while harnessing social network data for policy making. Similarly, the European research project PrimeLife[2] has developed a framework with which to analyze privacy issues related to other OSN users [4]. Project results show that privacy issues arise when legal or social norms are disregarded or technical safeguards are circumvented. Depending on the owner's initial categorization of personal data (private, semi-public, or public), the PrimeLife framework allows an estimation of 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,[3] another EU-funded project, conducted an in-depth study of privacy conceptualizations [5]. It takes a legal, social, economic, and ethical perspective of privacy, highlighting similarities and interdependencies. This project's results provide useful insights to help understand the concept of privacy; however, the analyses do not follow a structured approach, as described in this chapter.

3 Proposed Three-Layered Framework

In this section, we give an overview of our proposed framework. The framework provides a general-purpose structure for social web privacy research domains. Subsequently, the concept of privacy is broken up into a set of characteristics that are used to conduct our impact analysis, as described in Sects. 4 and 5.

3.1 Overview

In their conceptualization of privacy in 1890 as "the right to be let alone," Warren and Brandeis were one of the first to recognize the multidimensionality of the privacy concept [6]. Until then, privacy threats were primarily related to potential physical harm [7]. The rise of the information age led to a large number of privacy conceptualizations from a variety of directions such as the 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 from which to describe and analyze privacy [8]:

- *Legal*: This aspect focuses on laws and policies that protect the individual from corporations, governments, and other individuals. For example, the European

[1] http://www.padgets.eu/

[2] http://www.primelife.eu/

[3] http://www.prescient-project.eu/

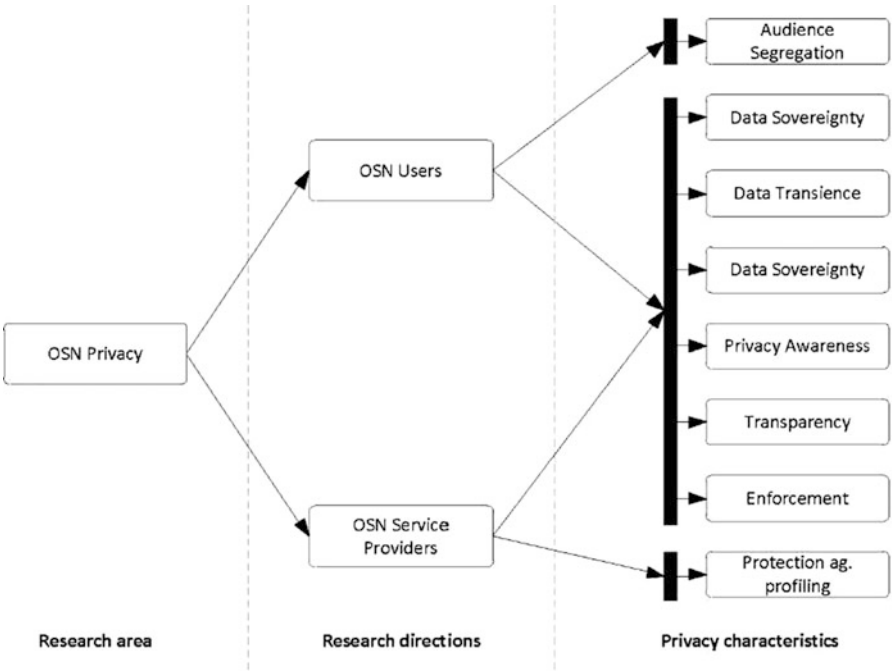

Fig. 1 Classification of OSN privacy research

Data Protection Framework promotes informational self-determination that emphases an individual's rights to control the collection and use of personal data [9].

- *Technical*: This aspect translates norms and regulations into technical specifications. The Platform for Privacy Preferences Project (P3P) is a popular example of enhancing the individual's ability to control information disclosure by technical means [10].
- *Social*: This aspect 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 [11]. Privacy is breached if personal information is available outside its intended context.

In this study, we adapt this three-layered view and extend it to cover privacy risks in online social networks. Typically, two distinct areas of research can be observed [12, 13] as depicted in Fig. 1:

- *OSN Service Providers*: Research in this direction includes the 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 [14].

Table 1 Proposed three-layered framework for analyzing social web privacy

	Privacy issues related to	
	OSN users	OSN service providers
Legal	International standards (Organisation for Economic Co-operation and Development (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

- *OSN Users*: This research aims to recreate the different social contexts of the real world; e.g., by supporting an individual to segment social streams for specific audiences, and by providing the means to have different digital identities [15].

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 1, with the cells containing concepts that become relevant for their respective dimension. Note that the three dimensions are not mutually exclusive – they are interdependent. In Sect. 3.2, the two research directions (OSN service providers and OSN users) are further decomposed into a set of privacy characteristics.

3.2 Characteristics Used to Analyze Social Web Privacy

This section outlines fundamental characteristics of privacy derived from a literature review. These privacy characteristics are not exhaustive; rather, they aim to provide a solid foundation for analyzing the impact of the three perspectives on privacy. The characteristics are described in detail as follows.

3.2.1 Data Sovereignty

Data sovereignty describes the extent to which an individual is able to control the processing of his personal data [16]; i.e., his informational self-determination. Personal data in an OSN is typically available in a structured manner and can easily be copied, linked, aggregated, and transferred [4]. Consequently, it is difficult for an OSN user to control the flow of personal information, and thus privacy is placed at risk. The problem increases because the OSN typically lacks the spatial,

social, and temporal boundaries of the real world, which limits the flow of personal information by default [17].

3.2.2 Data Transience

Data transience relates to the loss of personal information over time, which can be considered a typical characteristic of real-world communication [4]. In contrast, the mediated communication of OSNs results in permanent storage of personal information. As Mayer-Schönberger noted, "Since 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." [18]. In addition, this permanency of personal information poses a great challenge to privacy, since we are no longer free to construct our future identities because contradictory information may be available online [19].

3.2.3 Protection Against Profiling

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 [20]. Such profiling threats are increased if secondary data such as location (e.g. from mobile phones) and connection logs are linked to existing OSN profiles [21]. The relevance of these threats is underlined by sophisticated attacks such as stealing-reality attacks [22]. The current landscape of social web service providers, with their targeted advertising-centered business models and large identity silos, adds to this threat.

3.2.4 Audience Segregation

Originally developed by Goffman [23], audience segregation 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 intended for another audience, thereby keeping a consistent self-image and maintaining privacy [24]. 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.

3.2.5 Privacy Awareness

Privacy awareness encompasses the attention, perception, and cognition of the personal information others have received and how this information is or may be

processed [25]. An individual's awareness of privacy risk is a prerequisite for privacy-preserving behavior.

3.2.6 Transparency

With regard to OSN service providers, transparency describes the user's ability to be informed of processing and dissemination practices [26]. Taking a social point of view, transparency implies the ability of an individual to understand the flow of personal information within an OSN and to recognize contextual boundaries, which is important for contextual integrity [11].

3.2.7 Enforcement

Enforcement is 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 [27].

3.2.8 Summary

Figure 1 provides a summary of the presented characteristics of privacy. Most properties apply to privacy issues related to social web users and service providers; audience segregation only applies to the former, and protection against profiling only applies to the latter.

3.3 Classification Scheme

The analysis of each privacy characteristic is based on a structured scheme. First, legal aspects are analyzed, highlighting their impact on privacy issues related to OSN users and OSN service providers. Second, the effects of existing technical approaches for enhancing social web privacy are discussed. Finally, the implications of social norms on strengthening privacy in a given scenario are examined.

Additionally, for each privacy characteristic, a visualization of the classification and the effect is provided. A tripartite diagram is used to represent the legal, technical and social dimensions. In this diagram, a colored circle represents the impact (dark blue indicates a major impact, mid-blue a medium impact, and light blue a minor impact).

4 Privacy Issues Related to Social Web Users

In this section, we describe an impact analysis of privacy issues related to OSN users. The results are summarized in Sect. 4.7.

4.1 Data Sovereignty

From a legal point of view, laws and policies applicable to governing 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 in an attempt to strengthen data sovereignty. For example, access control models that enable the user to map their real world trust relationships to OSNs have been introduced [28]. Such technical approaches, in general, attempt to recreate real world social norms. Thus, they can be considered a useful means to strengthen data sovereignty, but 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 flow. 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 in the behavior of other users [20]. However, adherence to social norms highly depends on the trust relationship between two users, which are commonly divided into weak ties and strong ties [29]. Strong ties typically reflect relations with well-known acquaintances, and an abuse of confidence is likely to have a negative impact on the associated real-world relationship [29]. In contrast, studies indicate that users tend to have increasingly weak ties in OSNs, lacking fine-grained social relations [30], [20]. Individuals are commonly viewed as "contacts" or are even called "friends." Examining the impact on privacy issues related to other OSN users, unauthorized disclosure could primarily be regarded a social problem that relies on strong ties to be effective. As a consequence, the overall impact of the social aspect is medium, due to the aforementioned prevalent weak ties of current OSNs. Figure 2a illustrates our findings regarding data sovereignty.

4.2 Data Transience

Digitally mediated communication differs from real world communication; it adds persistence, searchability, replicability, and scalability by default [17]. However, other OSN users typically cannot be legally forced to delete voluntarily shared

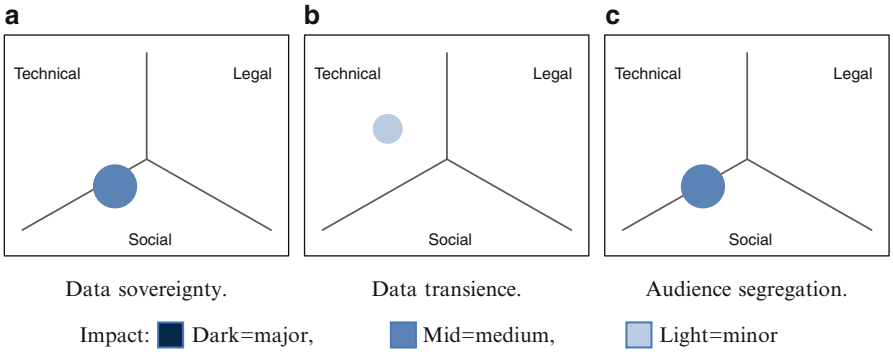

Fig. 2 OSN user privacy analysis (Part 1)

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 because digital information that is eventually available can easily be copied. While approaches to technical data transience exist, successful attacks, as demonstrated in [31], 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 existing data storage periods [20]. Consequently, we deduce a lack of social norms regarding data persistence, and conclude that there is no impact stemming from social aspects. A summary of our results is shown in Fig. 2b.

4.3 Audience Segregation

Managing the presentation of the self to different audiences is a social challenge that is not governed by legal regulations (no impact). From a technical perspective, audience segregation is partially implemented in common OSNs (e.g., Facebook Groups[4] and Google Circles[5]). In addition, audience segregation is starting to gain attention in the research community. The prototypical OSN Clique,[6] developed within the PrimeLife project, for example, implements a fine-grained access control mechanism to present each audience with a different view on a user's identity [24]. Another approach presented in [32] automatically determines distinct audiences based on the user's relationships. In the current state, a medium impact of audience

[4] http://www.facebook.com
[5] https://plus.google.com
[6] http://clique.primelife.eu/

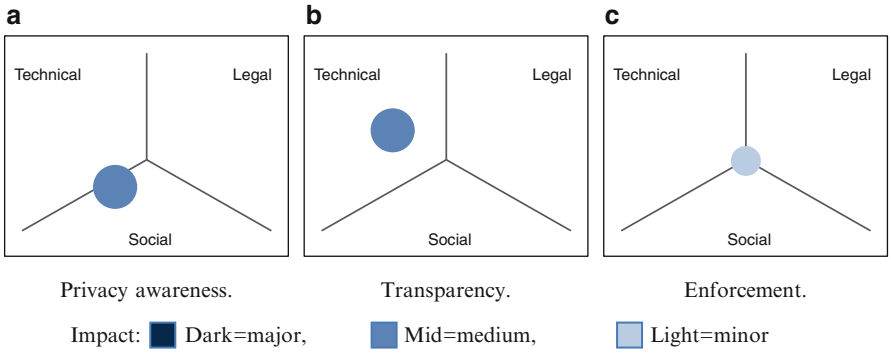

Fig. 3 OSN user privacy analysis (Part 2)

segregation on OSN user privacy can be deduced. However, increasing research activity indicates future growth of the importance of technical means.

From the social point of view, audience segregation is a useful concept that can be used to apply the theory of contextual integrity, as outlined in Sect. 3. Currently, however, audience segregation is not well supported in existing OSNs. Consequently, users resort to behavioral strategies such as choosing appropriate communication channels (e.g., private messages) and to mental strategies (e.g., self-censorship) [33]. Studies show that managing different audiences is a burden to many users, and is rarely applied [34]. Based on the results of the aforementioned studies, only a medium level of social impact of audience segregation on privacy can be inferred, as shown in Fig. 2c.

4.4 Privacy Awareness

Awareness is an important requirement of social web privacy that affects many of the characteristics presented in Sect. 3. However, from a regulatory point of view, OSN user awareness cannot be legally enforced (no impact).

Technical aspects such as usable user interfaces influence perceived privacy protection and the awareness of privacy risks [35]. However, similar to previous characteristics, technical aspects only have a supportive character with which to facilitate privacy awareness and draw attention to potential privacy violations (minor impact).

Privacy awareness is primarily a social concept with a gap existing between theoretical and practical privacy awareness [26]. Privacy awareness is backed by further studies indicating that OSN users frequently underestimate privacy risks and rarely use the available privacy settings [20, 36]. According to Acquisti, immediate gratification outweighs long-term privacy risk and leads to a myopic evaluation of privacy risks [37]. As illustrated in Fig. 3a, there is a medium level of social impact on privacy protection from other users due to the discrepancy between the theoretical and practical effects of privacy awareness.

4.5 Transparency

Although similar to privacy awareness, transparency aims to enhance a user's understanding of the propagation of personal data within an OSN to better protect the data from unauthorized access. From a legal perspective, an individual has few means with which to force other users to make their spreading of others' personal data transparent because, typically, no applicable regulations exist.

Taking a technical point of view, transparency-enhancing approaches focusing on logging and retrospective analysis of personal data disclosures have been proposed [38]. 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 [20]. Technical approaches to visually improving personal network transparency have been proposed, underlining that transparency strongly depends on the OSN service provider and related application programming interfaces (APIs) [39]. Following this reasoning, we assigned a medium level of technical impact because many transparency mechanisms rely on APIs that are 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. The results of our analysis of data transparency are shown in Fig. 3b.

4.6 Enforcement

The enforcement of law is an inherent property of any legal system. In the context of social web privacy, an individual can seek an injunction if reputation-damaging information is published. However, legal remedies 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 in order to be applicable [40]. In addition, legal remedies only allow the suing others after a privacy breach, thereby resulting in a minor overall impact of legal enforcement on privacy protection against other users.

A technical means of redress may have a positive impact on the enforcement of legal remedies. However, current OSNs differ widely in providing the technical means to address problems (e.g., cyber-bullying) [41]. Thus, technical means are considered to have only a supportive function with minor impact.

In 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 privacy interests [42]. Following the reasoning in [20] that relationships in OSNs often consist of weak ties, the effect of social norms on the enforcement of peer pressure can be considered minor. Figure 3c summarizes these findings.

Table 2 Summary of OSN user-related privacy impact analysis

	Data sovereignty	Data transience	Audience segregation	Privacy awareness	Transparency	Enforcement
Legal						
Technical						
Social						

Impact: Dark = major, Mid = medium, Light = minor

4.7 Summary

Table 2 summarizes the results of our impact analysis using the proposed framework. This section has described how 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 that influences privacy because the informational environment of OSNs is counterintuitive to the norms of personal data distribution in the real world. This often leads to a violation of contextual integrity [43]. Table 2 shows that technical approaches to privacy can be seen as a supportive means to translate social norms to the OSNs with 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 correspond to those of Strahilevitz, who suggested that the law does little to shape people's actual expectations of privacy [44].

5 Privacy Issues Related to Service Providers

Following the analysis of privacy issues related to social web users, we considered the impact of service provider-related privacy issues in this section. These results were then summarized and integrated into our framework.

5.1 Data Sovereignty

To ensure data sovereignty, legal norms have been enacted to control the exploitation of personal data by OSN service providers [40]. For instance, according to the German Teleservices Act and the Federal Data Protection Act, service providers require a user's explicit consent to use personal data for advertising purposes [40]. Furthermore, legal requirements for OSN service providers comprise the secure

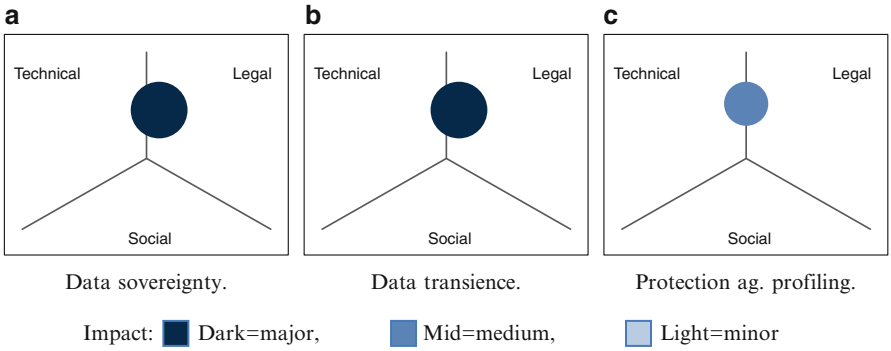

Fig. 4 OSN service provider privacy analysis (Part 1)

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. [14, 45]). 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 because their business model typically relies on free access to personal data for advertising purposes [4]. Hence, despite the theoretical effectiveness of the aforementioned approaches, the practical difficulties lead to only a medium level of 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 service provider adherence to data sovereignty. Therefore, there is no impact from this dimension. Figure 4a shows that data sovereignty with regard to OSN service providers is mainly legally driven with a medium level of technical influence.

5.2 Data Transience

Similar to data sovereignty, data transience is fully 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 [40]. Similarly, the European Data Protection Framework requires personal data to be removed if the purpose for which the data was collected ceases to exist [9]. This places the user in a strong position and leads to a high legal impact on data transience.

Approaches described in [31] can be applied to technically enforce data transience with respect to OSN service providers. However, their general impact can be

considered minor; in their general terms and conditions, most OSN service providers prohibit any tools that place access restrictions on personal data.

Similar to the description of data sovereignty (see Sect. 5.1), the missing social relationship between OSN users and OSN service providers leads to no social impact on the enforcement of data transience. This is illustrated in Fig. 4b.

5.3 Protection Against Profiling

Privacy threats stemming from OSN service providers have been recognized in the OECD privacy principles [46] and the EU Data Protection Framework [9], which stipulates that data minimization is one of the key principles preventing service providers from linking personal information and building digital dossiers. However, several of the underlying principles of the social web counteract data minimization. For example, 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 [41]. This leads to the conclusion that despite existing legal regulations to protect the user against profiling, the legal impact in practice can be considered minor.

Technically, the approaches presented in Sect. 5.1 can be applied to prevent profiling. Other research directions include the application of user-centric identity management systems on OSNs to strengthen user control, and to prevent service provider and third party access without prior approval. Maliki and Seigneur focused on the concept of Identity 2.0 and respective implementations [47]. They concluded that technical approaches in practice only have a minor impact on protection against profiling because 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). Figure 4c highlights the lack of social impact.

5.4 Privacy Awareness

Similar to user-related privacy threats (see Sect. 4.4), awareness is primarily influenced through a social perspective, while legal and technical means do not contribute at all.

For example, studies reveal that users of Facebook place more trust in the service provider than in average Facebook users [36]. They also show that 56 % believe that Facebook does not share personal information with third parties, and 70 % believe that Facebook does not combine information about them collected from other sources. Less than one out of four users claim to have read Facebook's privacy

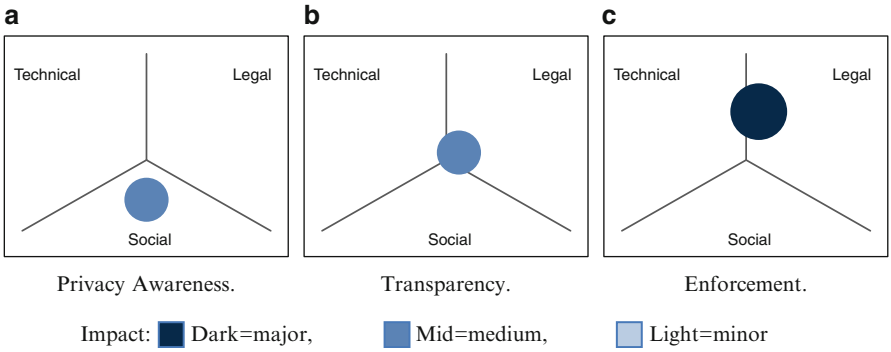

Fig. 5 OSN service provider privacy analysis (Part 2)

policy. While privacy risks tend to remain invisible to the average user [48], awareness increases if privacy-invading features are introduced such as Facebook's News Feed [49]. A high awareness is generally seen as a major obstacle in generating revenue by OSN service providers [12]. This leads to the conclusion that while awareness increases in exceptional situations, OSN users become accustomed to privacy threats stemming from service providers, thus leading to a medium social impact on privacy awareness (see Fig. 5a).

5.5 Transparency

The primary source of information used to assess the legal impact on transparency is the service provider's privacy policy. Bonneau and Preibusch extensively analyzed the privacy policies of 45 OSN providers [41]. 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 that is far too difficult for ordinary users to understand, have been identified. Other issues include a missing specification of applicable national data protection laws and the nation in which the data is stored and processed. These 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 revealed that users are often unable to determine the amount of personal data required prior to registration [26]. The study additionally shows that even upon request by e-mail, service providers often do not provide adequate support to increase the transparency of their data handling practices. Consequently, despite the existence of privacy policies as a valuable legal means of fostering transparency, there is only a medium legal impact due to the aforementioned restrictions in terms of practical implementation.

In addition to legal means, several technical approaches to service provider transparency have been developed. P3P is a prominent example [10]. P3P requires service providers to publish a machine-readable privacy policy that subsequently

can be matched with the user's predefined privacy preferences. However, most OSN service providers do not provide a machine-readable version of their privacy policy, thereby making P3P inapplicable [41]. Also, the task of defining privacy preferences can hardly be executed by non-technical users [50]. Taking these shortcomings into account, technical means have only a low impact on facilitating transparency.

Considering transparency from a social perspective, media coverage plays an important role in communicating the personal data handling practices of social web service providers [41]. However, they typically do not provide a substantive analysis of privacy problems; rather, they focus on partial aspects of privacy. The minor impact of mass media on transparency is also supported by the lack of privacy awareness (see Sect. 5.4). As illustrated in Fig. 5a, this leads to a minor overall impact of social means with respect to fostering transparency.

5.6 *Enforcement*

The inherent enforceability of legal measures (see Sect. 4.6) also applies to OSN service providers, and is reflected in the dominance of the aforementioned legal impact. OSN service providers typically employ a privacy-by-policy approach (e.g., as defined in [3]), notifying and obtaining the user's consent to its privacy policy prior to registration and thereby strengthening the legal impact of enforcing privacy interests (high impact).

Regarding the technical perspective, several means of enforcing OSN user privacy preferences are available (see Sects. 5.1 and 5.2). 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 toward other users (see Sect. 4.6), there is typically no social relationship between a social web service provider and its users. As a consequence, the power structures of social groups do not apply. In addition, the effect of mass media coverage is limited in its ability to put pressure on service providers, as outlined in Sect. 5.5. Thus, privacy interests toward service providers cannot be socially enforced (no impact). Figure 5a shows the dominance of legal remedies on the enforcement of privacy preferences.

5.7 *Summary*

Table 3 summarizes the results of our analysis of privacy issues related to OSN service providers. Two major conclusions can be derived. First, a shift of impact from the social dimension to the legal dimension, as compared to the results of Sect. 4, can be seen. Second, our results show a general increase in the impact of all

Table 3 Summary of OSN service provider-related privacy impact analysis

	Data sovereignty	Data transience	Protection ag. Profiling	Privacy awareness	Transparency	Enforcement
Legal						
Technical						
Social						

Impact: Dark = major, Mid = medium, Light = minor

dimensions compared to the impact of Sect. 4.7. In particular, the major legal impact is noteworthy and shows that legislators realize the existence of an unequal distribution of power. Consequently, they try to strengthen the position of OSN users. In contrast, the minor impact of social norms can be explained by a diffusion of responsibility. Service providers are typically not embedded in an individual's social structure; thus, social norms do not apply. Similar to the results described in Sect. 4.7, technical tools can be seen as a supportive in nature, although their impact is often limited. Finally, the limited means of all three dimensions to protect an individual against profiling is noteworthy, emphasizing the service providers' efforts to protect their business model.

6 Conclusion and Future Work

The rising popularity of online social networks poses many challenges in the field of privacy. Unlike the real world in which personal information is ephemeral, in the online-world, such information is almost infinitely available. This poses great challenges in managing identities online, and in 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 proposed an interdisciplinary approach to address the aforementioned privacy risks. Consequently, as the main contribution of this chapter, we developed a framework to systematically analyze social web privacy issues from a legal, technical, and social perspective. Furthermore, the impact of these 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. Our results support our initial assumption that the challenges of social web privacy cannot be addressed from a single direction; rather, they must be addressed by a comprehensive interdisciplinary approach.

Our results lead to a variety of research directions for future work. For example, the role of technology in pursuing social privacy violations should be investigated

in detail. Additionally, we wish to overcome the limitations of subjective and qualitative characterizations of privacy effects by conducting a quantitative study to investigate social web privacy based on the framework presented in this chapter. This could lead to a further convergence of research activities.

Acknowledgement The authors would like to thank Ludwig Fuchs (Department of Information Systems, University of Regensburg) for his helpful remarks and valuable suggestions to improve this work. This research was partly funded by the European Union under the FP7 PADGETS project (grant agreement no. 248920). The authors gratefully acknowledge this support. Any opinions, 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. Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. Bull Sci Technol Soc 11:544–564
2. Post RC (2001) Three concepts of privacy. Georget Law J 1:2087–2098
3. Spiekermann S, Cranor LF (2009) Engineering privacy. IEEE Trans Softw Eng 35(1):67–82
4. PrimeLife: D1.2.1 – Privacy Enabled Communities (2010)
5. Gutwirth S, Gellert R, Bellanova R, Friedewald M, Schiitz P, Wright D, Mordini E, Venier S (2011) Deliverable D1: legal, social, economic and ethical conceptualisations of privacy and data protection, Karlsruhe
6. Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4:193–220
7. Solove DJ (2006) A taxonomy of privacy. Univ Pa Law Rev 154(3):477560
8. Patil S, Kobsa A (2009) Privacy considerations in awareness systems: designing with privacy in mind. In: Markopoulos P, Mackay W, Ruyter B (eds) Awareness systems, human-computer interaction series. Springer, Heidelberg
9. European Parliament (1995) EU-Directive 95/46/EC. Official Journal of the European Communities
10. Cranor L, Dobbs B, Egelman S, Hogben G, Humphrey J, Langheinrich M, Marchiori M, Presler-Marshall M, Reagle JM, Schunter M, Stampley DA, Wenning R (2006) The platform for privacy preferences 1.1 (P3P1.1) specification. NOTE-P3P11-20061113
11. Nissenbaum H (2010) Privacy in context: technology, policy, and the integrity of social life. Stanford Law Books, Palo Alto
12. Ziegele M, Quiring O (2011) Privacy in social network sites. In: Trepte S, Reinecke L (eds) Privacy online. Perspectives on privacy and self-disclosure in the social web. Springer, Heidelberg/New York
13. Beye M, Jeckmans AJP, Erkin Z, Hartel PH, Lagendijk RI, Tang Q (2010) Literature overview – privacy in online social networks. Technical report TR-CTIT-10-36, centre for telematics and information technology, University of Twente, Enschede
14. Guha S, Tang K, Francis P (2008) NOYB: privacy in online social networks. In: Proceedings of the 1st workshop on online social networks, Seattle
15. van den Berg B, Leenes R (2011) Keeping up appearances: audience segregation in social network sites, Chap. 10. Springer, Dordrecht/Heidelberg, pp 211–231
16. Aimeur E, Gambs S, Ho A (2010) Towards a privacy-enhanced social networking site. In: Proceedings of the 5th international conference on availability, reliability and security, Corvallis
17. Boyd D (2008) Taken out of context: American teen sociality in networked publics. Ph.D. thesis, University of California, Berkeley

18. Mayer-Schonberger V (2009) Delete: the virtue of forgetting in the digital age. Princeton University Press, Princeton
19. Solove DJ (2008) The future of reputation: gossip, rumor, and privacy on the internet. Yale University Press, New Haven
20. Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the ACM workshop on privacy in the electronic society, New York
21. Hogben G (2007) Security issues and recommendations for online social networks. Technical report, ENISA
22. Altshuler Y, Aharony N, Pentland A, Elovici Y, Cebrian M (2011) Stealing reality: when criminals become data scientists (or vice versa). IEEE Intell Syst 26:22–30
23. Goffman E (1959) The presentation of self in everyday life. Anchor, New York
24. van den Berg B, Leenes R (2010) Audience segregation in social network sites. In: Proceedings of the 2nd international conference on social computing, Delft
25. Pötzsch S (2009) Privacy awareness: a means to solve the privacy paradox? In: Maty V, Fischer-Hübner S, Cvrcek D, Lvenda P (eds) The future of identity in the information society, IFIP advances in information and communication technology, vol 298. Springer, Heidelberg
26. Burghardt T, Buchmann E, Bohm K (2008) Why do privacy-enhancement mechanisms fail, after all? A survey of both the user and the provider perspective. In: Proceedings of the international workshop on web 2.0 trust, Trondheim
27. Carminati B, Ferrari E (2008) Access control and privacy in web-based social networks. Int J Web Inf Syst 4(4):395–415
28. Carminati B, Ferrari E, Perego A (2009) Enforcing access control in web-based social networks. ACM Trans Inf Syst Secur 13(1):1–38
29. Donath J, Boyd D (2004) Public displays of connection. BT Technol J 22(4):71–82
30. Boyd D (2004) Friendster and publicly articulated social networking. In: Proceedings of the SIGCHI conference on human factors and computing systems, Vienna
31. Federrath H, Fuchs KP, Herrmann D, Maier D, Scheuer F, Wagner K (2011) Grenzen des digitalen Radiergummis. Datenschutz und Datensicherheit – DuD 35(6):403–407
32. Netter M, Riesner M, Pernul G (2011) Assisted social identity management – enhancing privacy in the social web. In: Proceedings of the 10th international conference on Wirtschaftsinformatik, Zürich
33. Lampinen A, Tamminen S, Oulasvirta A (2009) 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, Sanibel
34. DiMicco JM, Millen DR (2007) Identity management: multiple presentations of self in Facebook. In: Proceedings of the international ACM conference on supporting group work, Sanibel Island
35. Grimmelmann J (2009) Saving Facebook. Iowa Law Rev 94(4):1137–1206
36. Acquisti A, Gross R (2006) Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Proceedings of the 6th workshop on privacy enhancing technologies, Cambridge
37. Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on electronic commerce, New York
38. Kolter J, Netter M, Pernul G (2010) Visualizing past personal data disclosures. In: Proceedings of the fifth international conference on availability, reliability and security, Krakow
39. Tscherteu G, Langreiter C (2009) Explorative Netzwerkanalyse im living web. In: Social semantic web. Springer, Berlin/Heidelberg
40. Dix A (2010) Daten- und Personlichkeitsschutz im Web 2.0. In: Klumpp D, Kubicek H, Rob Nagel A, Schulz W (eds) Netzwelt-Wege, Werte, Wandel. Springer, Berlin/Heidelberg, pp 195–210
41. Bonneau J, Preibusch S (2009) The privacy jungle: on the market for data protection in social networks. In: Proceedings of the 8th workshop on the economics of information security, London

42. Feldman DC (1984) The development and enforcement of group norms. Acad Manag Rev 9 (1):47–53
43. Peterson C (2010) Losing face: an environmental analysis of privacy on Facebook. SSRN eLibrary
44. Strahilevitz L (2005) A social networks theory of privacy. Univ Chic Law Rev 72(3):919–988
45. Baden R, Bender A, Spring N, Bhattacharjee B, Starin D (2009) Persona: an online social network with user-defined privacy. In: Proceedings of the ACM SIGCOMM conference on data communication, Barcelona
46. Organisation for Economic Co-operation and Development (1981) Guidelines on the protection of privacy and transborder flows of personal data, vol 11. Organisation for Economic Cooperation and Development, Paris
47. Maliki TE, Seigneur JM (2009) Identity management. In: Vacca JR (ed) Computer and information security handbook, Chap. 17. Burlington, Morgan Kaufmann
48. Debatin B, Lovejoy JP, Horn AK, Hughes BN (2009) Facebook and online privacy: attitudes, behaviors, and unintended consequences. J Comput-Mediat Commun 15(1):83–108
49. Hoadley CM, Xu H, Lee JJ, Rosson MB (2010) Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry. Electron Commer Res Appl 9 (1):50–60
50. Agrawal R (2002) Why is P3P not a PET? In: Proceedings of the W3C future of P3P workshop, Dulles

http://www.springer.com/978-1-4614-4138-0

Security and Privacy in Social Networks

Altshuler, Y.; Elovici, Y.; Cremers, A.B.; Aharony, N.;
Pentland, A. (Eds.)

2013, VI, 254 p., Hardcover
ISBN: 978-1-4614-4138-0