Privacy in Social Collective Intelligence Systems

Simone Fischer-Hübner and Leonardo A. Martucci

1 Introduction

In this chapter we discuss privacy, a fundamental human right, in Social Collective Intelligence Systems (SCIS). Privacy is a key non-functional requirement related to the right of individuals to control information related to them. The fundamentals of SCIS are based on basic concepts such as profiling, provenance, evolution, reputation and incentives. This chapter discusses the impact of such concepts on the individual right to privacy. It also discusses that while, on the other hand, SCIS have some inherent characteristics that can be utilized to promote privacy, still several technical challenges remain. Both privacy laws as well as privacy-enhancing technologies are needed to effectively enforce privacy.

This chapter is organized as follows. The concept of privacy is introduced in Section 2 and relevant basic privacy principles of the European Data Protection Legal Framework and the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines are presented in Section 3. The risks to privacy, mainly in terms of profiling, provenance, trust and reputation in SCIS are listed in Section 4. Then, the opportunities provided by the design of SCIS that can help to promote privacy as well as related technical challenges are discussed in Section 5. Section 6 outlines legal privacy rules provided by the European Data Protection Legal Framework in regard to profiling and Section 7 presents a selection of privacy-enhancing technologies that can technically enforce the basic privacy principles in SCIS. Finally, Section 8 briefly summaries the main findings and open research challenges.

Simone Fischer-Hübner
Karlstad University, 651-88 Karlstad, Sweden. e-mail: simone.fischer-huebner@kau.se

Leonardo A. Martucci
Karlstad University, 651-88 Karlstad, Sweden. e-mail: leonardo.martucci@kau.se

2 Concept of Privacy

Privacy is a core value and is recognized either explicitly or implicitly as a fundamental human right by most constitutions of democratic societies. In the end of the 19^{th} century, the American lawyers Warren and Brandeis defined privacy as the "right to be let alone" [45]. Another definition from the early years of computing is by Alan Westin, who defined privacy as the "the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [47].

In general, the concept of personal privacy has several dimensions, including the dimensions of informational privacy (by controlling whether and how personal data can be processed or disseminated – see also Westin's definition), territorial privacy (by protecting the close physical area surrounding a person) and privacy of a person (by protecting a person against undue interferences) [20]. In the context of Social Collective Intelligence, the aspect of informational privacy will be the most relevant one and will thus also be the focus of our discussion.

Privacy, however, is not an absolute right, as it can be in conflict with rights of others or other legal values, and because individuals cannot participate fully in society without revealing personal data. Nevertheless, in cases where privacy has to be restricted, the very core of privacy still needs to be protected. Therefore, privacy and data protection laws, as those ones implementing the EU Data Protection Directive 95/46/EC [17], have the objective to define fundamental privacy principles that need to be enforced if personal data is collected, stored or processed. Such fundamental privacy principles will be discussed in the next section.

The EU Data Protection Directive 95/46/EC and most other privacy and data protection laws and guidelines only apply if *personal data* are processed, which are defined by Art. 2 of the Directive as "any information related to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity;".

The Opinion 4/2007 of the Article 29 Working Party[1] contains an analysis of the concept of personal data described in the EU Data Protection Directive 95/46/EC. Among its conclusions and clarifications, the Working Party noted that data relates to an individual if it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. For instance, data that is related to the individuals behavior profiled under RFID tag identifiers associated to them or the MAC addresses of their smartphone wireless interfaces is personal data, even though these individuals may not be known or identified by their names. The Opinion 4/2007 of the Article 29 Working Party also states that natural persons are 'identified' when, assuming that

[1] The Article 29 Working Party consists of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission.

they are part of a group of persons, they are distinguished from all other members of the group.[2]

3 Basic Privacy Principles

In this section we provide an overview to internationally accepted, basic legal privacy principles, which are part of the general EU Data Protection Directive 95/46/EC [17] and need also to be addressed by SCIS. The Data Protection Directive has been an important legal instrument for privacy protection in Europe, as it codifies general privacy principles that have been implemented in the national privacy laws of all EU member states and of many other states. The principles also correspond to principles of the OECD Privacy Guidelines [36] to which we will also refer to.

1. **Legitimacy:** Personal data processing has to be legitimate, which is according to Art. 7 EU Directive 95/46/EC usually the case if the data subject has given his unambiguous (and informed) consent, if there is a legal obligation, or contractual agreement (cf. the Collection Limitation Principle of the OECD Guidelines).
2. **Purpose specification and purpose binding:** Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with these purposes (Art. 6 I b EU Data Protection Directive 95/46/EC — cf. Purpose Specification and Use Limitation Principles of the OECD Guidelines).
3. **Data minimization:** The processing to personal data must be limited to data that are adequate, relevant and not excessive (Art. 6 I (c) EU Data Protection Directive 95/46/EC). Besides, data should not be kept in a personally identifiable form any longer than necessary (Art. 6 I (e) EU Data Protection Directive 95/46/EC – cf. Data Quality Principle of the OECD Guidelines, which requires that data should be relevant to the purposes for which they are to be used). In other words, the collection of personal data and extend to what personal data are used should be minimized, allowing for instance users to act anonymously or pseudonymously. Obviously privacy is best protected if no personal data at all (or at least as little data as possible) are collected or processed.
4. **Restriction for the processing of sensitive data:** According to Art. 8 EU Data Protection Directive 95/46/EC, the processing of so-called special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or aspects of health or sex life are generally prohibited, subject to exceptions (such as explicit consent).

[2] The Article 29 Working Party statement is close to the definition of anonymity from Pfitzmann and Hansen [37]: “anonymity of a subject from an attackers perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set” , which is commonly used in the computer security and privacy area.

5. **Transparency and Rights of the Data Subjects:** Transparency of data processing means informing a data subject at least about the data processing purposes as the identity of the data controller[3] as well as further information, such as information about the possible recipients of the data and the rights and controls of the data subject.[4] The EU Data Protection Directive 95/46/EC provides data subjects with respective information rights according to its Art. 10. Further rights of the data subjects include the right of access to data (Art. 12 (a) EU Directive 95/46/EC), the right to object to the processing of personal data (Art. 14 EU Directive 95/46/EC), and the right to correction, erasure or blocking of incorrect or illegally stored data (Art. 12 (b) EU Directive 95/46/EC, cf. Openness and Individual Participation Principle of the OECD Guidelines).
   Of special interest for SCIS are data subject rights in the context of automated decisions that are, for instance, made based on profiling. According to Art. 12 (a) EU Directive 95/46/EC, the right to access data includes the right to obtain from the data controller "knowledge of the logic involved in any automatic processing of data concerning the data subject at least in the case of the automated decisions". Pursuant to Art. 15 (1) EU Directive 95/46/EC, individuals have in principle "the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."
6. **Security of data processing:** The data controller needs to implement appropriate technical and organizational security mechanisms to guarantee the confidentiality, integrity, and availability of personal data (Art. 17 EU Directive 95/46/EC — cf. Security Safeguards Principle of the OECD Guidelines);

In January 2012, the EU Commission published a proposal for a new EU General Data Protection Regulation (GDPR) [18], which defines a single set of modernized privacy rules, and which will (once the regulation will be in force) be directly valid across the EU. On October 12, 2013, the LIBE Committee (Committee on Civil Liberties, Justice and Home Affairs) of the European Parliament voted on compromise amendments to the GDPR [16]. In particular, it includes the principle of data protection by design and by default (Art. 23), requiring building privacy enhancing technologies (PETs) already into the initial system design. Besides, the requirements of transparency of data handling by *concise, transparent, clear and easily accessible policies* (Art. 11) is explicitly stressed. Moreover, the right to erasure is newly introduced in Art. 17 (which was initially branded as the right to be forgotten in the GDPR from January 2012).

Important in the context of Social Collective Intelligence are also newly introduced rules on profiling (Art. 20), including the data subject's right to object to profiling as well as prohibition of profiling that has a discriminatory effect on the

[3] According to EU Data Protection Directive 95/46/EC, a data controller is defined as the entity that alone or jointly with others determines the purposes and means of personal data processing.

[4] According to EU Data Protection Directive 95/46/EC, a data subject is a natural person about whom personal data are processed has in regard to his personal data.

grounds of race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, sexual orientation or gender identity. “The controller shall implement effective protection against possible discrimination resulting from profiling” (see further discussion below).

Even though the GDPR and its amendment are not enacted yet, it contains legal principles that have been broadly accepted as being important for the protection of privacy in the future.

4 Risks to Privacy in Social Collective Intelligence Systems

SCIS are based on technical concepts, such as profiling, reputation and incentives systems, and data provenance, which all may require the collection and processing of personal data and thus pose privacy risks. Some specific privacy risks related to these technical concepts will be discussed in this section.

4.1 Profiling

Profiles are sets of data that portray significant features of a subject. It aims to represent the extent to which an individual exhibits traits or abilities as determined by tests or ratings [34]. Data used to build profiles are mainly taken from individual’s input, which is either explicitly or implicitly revealed or implicitly derived. The explicitly revealed data relate to information and statements that individuals directly disclose about themselves. The implicitly revealed data relate to information that is (automatically) gathered from supervisory systems or sensors that track the activities of individuals. Implicitly derived data are additional data that can be inferred from the data set and it is not produced or collected from individuals. It usually relates to results from statistical analysis on the data set. For instance, social networks contain explicitly revealed data posted by their users; loyalty programs collect data from customers’ shopping or traveling activities, i.e. implicitly revealed data, and both social networks and companies running loyalty programs implicitly derive data about the customer habits.

Profiling affects privacy in different respects. As the Council of Europe has discussed in its recommendation CM/REC(2010)13 on profiling [10], the collection, linking, calculation, comparison and statistical correction of data with the objective to create profiles may have significant privacy impacts, as profiling enables a person’s personality, behavior, interests and habits to be determined, analyzed and/or predicted. Often such profiling is even happening without the knowledge of the individuals concerned. While profiling may offer benefits for users and society at large, e.g. by providing users with targeted and better services addressing personal and societal interests or by permitting an analysis of risks and fraud. Profiling techniques can also have a negative impact on the individuals concerned by placing them in

predetermined categories that may unjustifiably deprive them from accessing certain services and by this discriminate individuals [10].

Moreover, as mentioned above, profiling techniques do not only allow to analyze data that are actually recorded, but also allow to statistically predict or implicitly derive personal information from such records. For instance, it has been shown that sensitive data including political opinions, religious beliefs, intelligence or sexual orientation can be automatically predicted from Facebook Likes (see e.g., [28]).

For these reasons, it is important to protect privacy rights of individuals subject to profiling both by law and technology. Legal rules and privacy enhancing technologies for protecting the user's privacy will be discussed in the subsequent sections.

4.2 Provenance and Reputation

Reputation is a result of past interactions within a given context [12]. Reputation systems help users to select providers offering competing services. Obtaining a good reputation is a powerful incentive for service providers because the better their reputation is, the more services can delivered or a higher premium can be gained. Hence, both service consumers and providers benefit from reputation systems.

In reputation systems, sequences of past interactions are linked to a subject and the aggregated quality of such interactions is used to determine the reputation of the subject. Provenance is therefore needed to correctly associate an interaction to a subject consuming a service and the service to a service provider. Thus, the correct identification of subjects and services is fundamental for provenance. The process of identification naturally requires some sort of identifier and, in the case of reputation systems and provenance in general, these identifiers are needed to be long-term identifiers because a history of past actions is going to be associated to them.

However, having numerous transactions linked to a single long-term identifier potentially reveals customs and habits of data subjects, i.e., personal data. In addition, decision-making based on reputation systems can be based on direct and indirect interactions, i.e., opinions from other users. Expressing one or multiple opinions about a service can potentially reveal personal information about the users' habits and lead to profiling. Users could then refrain by providing feedback but that would reduce the usefulness of the reputation system. Therefore, privacy in reputation systems has to be considered from the perspective of users providing services and of users consuming services.

From the data protection perspective, short-term identifiers, such as transactions pseudonyms [37], i.e., pseudonyms that are used only once, are able to better protect the privacy of data subjects because their multiple transactions are not easily linked but that would weaken the security of the reputation system, as it could be easily abused. There is a clear conflict between a key requirement of reputation services, i.e., keeping histories of interactions, and general privacy goals, i.e., keeping transaction records unlinkable. Reputation, which is an intrinsic type of incentive,

and privacy are core aspects of SCIS that are required to co-exist. Therefore, this notional dissonance needs to be addressed and it is further discussed in Section 7.5.

5 Technical Opportunities and Challenges for Protecting Privacy

While SCIS pose different types of privacy risks as we have discussed above, they also have inherent characteristics, such as distribution, hybridity, and the focus on collectives instead of individuals only, which can be utilized for a privacy-enhanced system design. This section discusses opportunities and challenges for designing a privacy-preserving system that takes into account the inherent characteristics and technical concepts of SCIS.

5.1 Formation of Collectives and Privacy

Social collective intelligence is based on hybrid systems, where humans and machines compose and closely cooperate as a collective to solve challenging tasks. A key feature of SCIS is the utilization of group intelligence by composing the "right" collective (or set) of humans and machines that is suitable for the solving a given task.

The formation of collectives is related with privacy from two main directions. First, from the anonymity perspective, we evaluate how peers (humans), which are part of collectives, can remain anonymous. Second, from the identity management perspective, we present how collectives can be used for audience segregation and for handling multiple partial identities.

5.1.1 Collectives and Anonymity

The peer profile of a larger collective may not classify as personal data, if the collective is formed in such a way that it does not relate to any identified or identifiable person, i.e., if the individuals of the collective are anonymous and devices that are part of the collectives do not provide personal data. In this case, privacy of individuals is not affected and privacy laws do not apply.

As privacy will be best protected if no personal data are processed at all or if personal data cannot be directly attributed to the data subjects, research challenges to be addressed also include the question how peer profiles can be anonymized or pseudonymized, and/or how peer profiles of collectives can be formed in an anonymous manner.

One leading principle for the formation of collectives in SCIS is diversity [4]. For instance, diversity in opinions helps to eliminate decision bias in collectives and promote different viewpoints. The notion of diversity is also a key component in

anonymity metrics, i.e., standards of measurements that aim at quantifying the level of privacy of a subject. Anonymity means that a subject is not identifiable within a set of subjects (the anonymity set) who might have caused a given action [37] or associated to a given piece of information [43]. The cardinality of the anonymity set can be used as a simple privacy metric.

Diversity has a strong impact, either positive or negative, on the privacy of subjects. First of all, diversity decreases the homogeneity of the set of subjects and, thus, may also reduce the cardinality of anonymity sets and the level of privacy for the subjects (persons) that are elements of these sets. The anonymity set size is related to another metric, the k-anonymity.

K-anonymity [43] is a formal privacy protection model that aims at preventing the re-identification of individuals in a given person-specific field-structured data (structured database) while maintaining the utility (usefulness) of the data. The idea behind *k*-anonymity is that a record from a database is released only if there are at least $(k-1)$ other similar records, i.e., whose values of quasi-identifiers are indistinguishable from the each other. Thus, there are at least k subjects that can be linked to a given release of data. In addition, *k*-anonymity can be used to quantify anonymity in location-based services, as shown in [25, 22].

L-diversity [30] is a model that extends *k*-anonymity. It proposes a solution for the blindness of k-anonymity regarding diversity in sensitive information that can be exploited using attacks that use public (non-sensitive) information to obtain sensitive information. The idea behind *l*-diversity is that the diversity of sensitive attributes has to be at least l (where $l > 1$). Therefore, lack of diversity of sensitive attributes can also negatively affect privacy.

T-closeness [29] extends *l*-diversity by proposing restrictions to the disclosed sensitive data, which should follow the distribution of the overall table. Differential privacy [15] is a formal model that ensures that addition or removal of single items of a database does not significantly affect the outcome of an analysis. Differential privacy shows that any statistical database that releases data with a non-trivial utility also leaks personal information. Differential privacy also offers means to quantify the level of loss of personal information against the utility of the data retrieved from the database. Data mining with formal privacy guarantees based on differential privacy is described in [21].

While anonymity is hard to guarantee and hard to measure, still the approaches and metrics mentioned above could help to compose collectives that also form suitable anonymity sets.

5.1.2 Collectives and privacy-enhancing Identity Management

Peers can take part in multiple collectives and provide different contributions in terms of knowledge and skills to each collective. In principle, this also allows one human to be represented by different (partial) identities in different collectives or to be represented in one collective with different agents, which represent different (partial) identities of the user in dependence on the current context.

The sociologist Erving Goffman described the concept of audience segregation, meaning that people usually play different roles in different situations and perform differently for different audiences [24]. Privacy-enhancing identity management systems [7] technically enforces audience segregation by allowing users to selectively disclose subsets of their personal data, so-called partial identities, under different pseudonyms to different communication partners dependent on their current context.

While establishing multiple identities prevents users and their agents from being completely profiled under one identity and thus promotes privacy, it also enables compromises by so-called Sibyl attacks. A Sybil attack is an identification attack that occurs when a malicious user influences the network by controlling multiple logical identifiers from a single physical device. In a Sybil attack, malicious users assume multiple identifiers, preventing the usage of security mechanisms based on filters, reputation or trust assumptions [14]. In [32], the concept of self-certified Sybil-free pseudonyms is presented, which allows protecting against Sybil attacks on distributed systems in a privacy-friendly manner.

5.2 Distribution for promoting Privacy

While centralized systems and collections of data pose privacy risks due to data mining and potential data leakages, Decentralized Systems and Services for Privacy Preservation, such as online social networks, private data storage and backup, or anonymous content dissemination and communication systems, have been developed and researched in the recent years that are removing the need for a powerful centralized provider with its knowledge (see [5]).

Examples are peer-to-peer anonymous communication mechanisms, such as Crowds [41] and Chameleon [31], which are run by the collective of users and based on the compositionality of individual interactions [23]. Tor [13], the most relevant anonymous communication system, is also supported and run by collective that voluntarily offers networking and computing resources to provide anonymity to Internet users.

Online social networks can aggregate collectives and are potential important means for providing compositionality between collectives and machines, as the social networks provide an invaluable source for machines to learn from people. Safebook [11], Peerson [6], and Diaspora are distributed peer-to-peer privacy-friendly online social networks that were proposed and lately implemented.

The distributed nature of SCIS can potentially also be utilized for distributing knowledge and power and thus promoting privacy.

6 Legal Privacy Protection for Profiles

This section discusses how legal privacy rules that are enacted by the EU Data Protection Directive 95/46/EC or proposed as part of the GDPR and its compromise amendment can help to enforce privacy. As reputation scores and personalized incentives schemes [23] can also be viewed as profiles, this section focuses on legal means for protecting personal data of profiles in the form of peer profiles, reputation and incentives schemes.

If a profile contains personal data, then restrictions apply to the propagation or exchange of profiles according to the European data protection legislation. However, if a profile is anonymized and does not contain any personal data, the Directive 95/46/EC does not apply, as its Recital 26 states that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." In practice, the question whether data is anonymous or not is very difficult to answer. This particularly applies to statistical data, "where despite the fact that the information may be presented as aggregated data, the original sample is not sufficiently large and other pieces of information may enable the identification of individuals." For instance, data sets published by AOL, a media company, and by Netflix, a provider of on-demand streaming media, in 2006 that were claimed to be anonymized were later proven not to be since a number of individuals could be re-identified from the data set (see [35]). The Recital 26 demands that for deciding whether data is anonymous "all the means likely reasonably to be used either by the controller or by any other person" should be taken into account.

Basic legal privacy principles, especially those enacted by the EU Data Protection Directive 95/46/EC and the proposed GDPR (cf. section 3), need to be enforced when profiles including personal data are created and processed:

- The collection and processing of personal data in profiles needs to be *legitimate*, which usually implies that the data subjects have given their informed consent (Art. 7 — Legitimacy & informed consent).
- Personal data used in the context of profiling must be collected for *specified and legitimate purposes* and may later *only be used for those purposes* (Art. 6 Ib — Purpose specification & binding).
- Furthermore, the amount of personal data and the extent to which they are collected and processed in profiles should be *minimized* (Art. 6 Ic — Data minimization), which implies that if possible data in profiles should be *anonymized* or *pseudonymized*.
- The collection and processing of *so-called special categories of data* in the context of profiling should in principle be *prohibited* (Art. 8 I — No sensitive data), unless the exceptions of Art. 8 II apply.
- Data controllers have to provide the data subjects with sufficient *privacy policy information* pursuant to Art. 10 when personal data are collected in the context of profiling. Data subjects that are being profiled have the right to access (i.e. to obtain information about) their personal data as well as the right to be informed by the data controller about the logic underpinning the processing of their profile

data. Furthermore, data subjects have *rights to correction, deletion and blocking of their data*, as well as the *right not to be subject to a "decision which produces legal effects concerning him or significantly affects him and which that is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."* (Transparency & data subject rights).

- The data controller has to implement proper *technical and organizational security measures* for the protection of personal profile data (Art. 17 — Security).

The Council of Europe has in an appendix to its recommendation CM/REC(2010)13 proposed more specific privacy principles that should further strengthen the data subject's protection.

In the context of the EU Data protection reform, the newly proposed General EU Data Protection Regulation (GDPR) [18] introduced with its Art. 20 "Measures based on Profiling". This was however criticized by the Article 29 Data Protection Working Party on focusing merely on the outcome of profiling rather than on the profiling as such [3]. The Article 29 Data Protection Working Party therefore demands a comprehensive approach that also includes legal requirements for the purpose of profiling and the creation of profiles as such, referring to the principles of the appendix to Council of Europe recommendation.

The compromise amendment to the proposed EU Data Protection Regulation [16], which was passed by the LIBE Committee of the European Parliament on October 21, 2013, has taken up this proposal by providing greater transparency and control for data subjects. According to the amended Art. 14 (ga), data controllers should provide "information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject". Besides, the amended proposal includes the right for data subjects to object to profiling (Art. 20 I). Furthermore, pursuant to Art. 20 III, "profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited". Pursuant to Art. 20 V, "Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment."

The GDPR defines 'profiling' as "any form of automated processing of personal data intended to evaluate certain personal aspects relating to *a natural person* or to analyze or predict in particular *that natural person's* performance at work, economic situation, location, health, personal preferences, reliability or behavior". Thus, the GDPR and its amendment text refer to profiles comprising data about one individual. However, if profiles contain personal data of several individuals or data that relate to several individuals, the enforcement of the legal rules in regard to consent, transparency and data subject rights discussed above may be practically more difficult to enforce — especially if the data subjects concerned have conflicting interests in regard the transparency, confidentiality or retention of their data.

The amendment text to the GDPR also introduced in Art. 4 (2a) the concept of "pseudonymous data", defined as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution." Recital 58a of the amendment, further states that profiling based solely on the processing of pseudonymous data that cannot be attributed to a specific person should be presumed not to significantly affect the interests, rights or freedoms of the data subject.

The Article 29 Working Party is also pointing out the need for more responsibility of the data controllers. In particular, a data protection impact assessment as foreseen in Art. 33 of the GDPR needs to be conducted as a basis for suitable safeguards for profiles comprising privacy enhancing technologies and privacy friendly default settings (cf. Art. 23 of the GDPR on Data Protection by Design and by Default.

In conclusion, peer profiles relating to individuals may raise privacy concerns. Therefore, suitable legal and technical measures to protect the data subject's rights to information self-determination are needed. While the basic privacy principles of the EU Directive 95/46/EC are implemented by the national laws of the EU member states, the more advanced principles of the proposed EU regulation and its amendment are not finally enacted yet. Still, they reflect important requirements set up by privacy experts and decision makers and are expected to pass as part of the Regulation in this or similar form at least.

The privacy principles discussed above can be enforced more effectively by SCIS and applications by following a Privacy by Design approach. In section 7, we will discuss privacy enhancing technologies for technically enforcing basic privacy principles.

7 Privacy-Enhancing Technologies

In this section, we present a selection of privacy-enhancing technologies (PETs) and show how they can be used to technically enforce basic privacy principles.

7.1 Anonymous Credentials

Anonymous credential protocols are key technologies for enforcing data minimization for applications.

A traditional credential (often also called certificate or attribute certificate) is a set of personal attributes, such as birth date, name or address, signed (and thereby certified) by the certifying party (the so-called issuer) and bound to its owner by cryptographic means. Traditional credentials require, however, that all attributes are disclosed together if the user wants to prove certain properties, so that the verifier can check the issuers signature. This makes different uses of the same credential

linkable to each other. Besides, the verifier and issuer can link the different uses of the users credential to the issuing of the credential. Anonymous credentials allow the user to essentially "transform" the certificate into a new one that contains only a subset of attributes of the original certificate, i.e. they allow proving only a subset of its attributes to a verifier (selective disclosure property). Instead of revealing the exact value of an attribute (e.g., the exact birth date or address), anonymous credential systems also enable users to apply any mathematical function to the (original) attribute value, allowing them to prove only attribute properties without revealing the attributes themselves (e.g., one may only reveal the fact that she or he is over 18 and/or lives in Trento — which may be sufficient for authorizing a service). In addition, the Idemix protocol by Camenisch et al. [8], which is an implementation of anonymous credentials, allows the issuer's signature to be transformed in such a way that the signature in the new certificate cannot be linked to the original signature of the issuer. Hence, different credential uses cannot be linked by the verifier and/or issuer (unlinkability property).

7.2 Transparency Enhancing Tools

As mentioned in Section 3, transparency of personal data processing for data subjects is a basic privacy principle, and consequently the Legal European Data Protection Framework grants data subjects rights to information for making the processing of their data transparent.

Transparency-enhancing tools (TETs) provide technical means for enforcing these data subject rights. According to [27], TETs can be divided into ex ante TETs which enable the anticipation of consequences before data is actually disclosed, and ex post TETs which inform about consequences if data already has been revealed. Examples for ex ante TETs are privacy policy languages, such as P3P [44] or PPL [38], which could also be used in the context of SCSI for informing users more transparently about privacy policies, e.g. when they have to provide their informed consent to disclose personal data for peer profiling or other purposes.

Ex post TETs comprise tools that provide data subjects with online access to their data at the service provider's side [46] or access to logs documenting how their data were processed. As logs that are recording who has accessed data and how the data has been processed in turn also include personal data (e.g., the fact that a medical record of a patient has been accessed by a psychiatrist reveals sensitive personal information), they have to be designed in a privacy-friendly manner. Privacy preserving transparency logging schemes are for instance introduced in [39, 26]. They propose methods for the encryption of log records in such a way that the records are only accessible by the data subjects to which the records relate.

7.3 PrimeLife Policy Language (PPL)

Machine-readable privacy policy languages have the objective to make privacy policies of services sides more transparent, negotiable and enforceable. Compared to hard-coded fixed policies, they provide more flexibility, as they allow to easily express, change and extend privacy policies without the need to reimplemented the system that enforces the policy. Besides, if the language is agreed-upon or standardised, privacy policies can easily be communicated across interacting entities in different domains [38].

The PrimeLife Policy Language (PPL) for privacy-enhanced access control and data handling was developed in the EU FP7 project PrimeLife [38], and is based on two widespread industry standards, XACML (eXtensible Access Control Markup Language) and SAML (Security Assertions Markup Language). PPL is a language that allows to specify privacy policies of data controllers as well as privacy preferences of users (who are the data subjects in this case), which can be matched to check whether a data controller's policy complies with a user's preferences.

Let's consider the scenario depicted in Figure 1 involving a data controller requesting personal data from a user. The data controller may later want to forward the personal data to a third party, a so-called downstream controller.

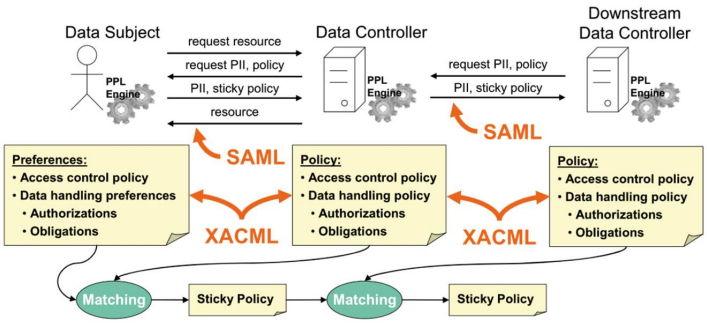

Fig. 1 Matching the data subject's privacy preferences and the data controller's privacy policy [38].

The data controller sends the data request to the user together with a privacy policy, which consists of an access control policy, specifying what information he needs from the user, and a data handling policy specifying how he will treat the revealed data. PPL allows specifying both uncertified data requests as well as certified data requests based on proofs of the possession of (anonymous Idemix [8] or traditional X.509) credentials that fulfill certain properties. The data handling policy is expressed in terms of authorizations, e.g., for what purposes the data will be used, and obligations that the data controller is willing to fulfill for collected data items (e.g., to delete the data after a certain time period or to log all accesses to the data).

Similarly, the data subject's privacy preferences specify to which data controller and downstream data controllers each data item can be released and how users expects their data to be treated.

The PPL engine conducts an automated matching of the data controller's policy and the user's preferences, which can result in a mutual agreement concerning the usage of data in form of a so-called "sticky policy", which should "stick to the data" and be stored and enforced at the data controller side (by the XACML access control engine). If data are to be forwarded to third parties (downstream data controllers), the data's sticky policy is first matched with the downstream controller's policy, which may result in a new sticky policy traveling with the data for enforcement at the downstream controller's side.

PPL extends XACML, so that the language can express both data subject's preferences and the (downstream) data controller's policies. Besides, concept of (anonymous Idemix) credential-based access control was integrated in PPL. For the communication between the different parties, SAML was extended to communicate credential-based attribute proofs and to attach sticky policies to the revealed attributes. Privacy policy languages such as PPL can be used to protect the access to personal data contained in peer profiles according to the user's preferences.

7.4 PETs for protecting peer profiles

PPL and other PETs as presented above can help to technically enforce the main legal privacy principles derived from the European Legal Data Protection Framework in regard to peer profiling:

- **Informed consent:** With PPL, a consent form including a short privacy notice can be displayed to the user before the user discloses personal data from his peer profile, informing him about the main aspects of the data controller's privacy policy and about how far it matches with his privacy preferences. Only if the user provides his consent, there will be a valid agreement (in form of a sticky policy) and data will be disclosed. (For proposals of usable PPL user interfaces for obtaining informed consent, please refer to [2]);
- **Purpose specification & binding:** With PPL, the data controller's privacy policy can clearly state the purposes for which requested personal data items will be used. The XACML access control engine will enforce that personal data can only be accessed for the agreed upon sticky policy. This means that the use of data will be restricted to the purposes stated in the sticky policy;
- **Data minimization:** PPL allows the user to disclose certified data in form of anonymous credential proofs, which can via their selective disclosure and unlinkability properties enforce data minimization on application level. Furthermore, obligations, which a user and data controller have agreed upon, in regard to the data retention period can help to minimize the life time of personal data;
- **Transparency:** As discussed above, privacy policy languages can make it more transparent to users how far a data controller's policy matches their privacy pref-

erences before they disclose personal data (ex ante transparency). Ex post transparency of how data are processed (once they have been disclosed to a data controller) can be enforced by agreeing on obligations that a service provider needs to fulfill. For instance, those obligations may include notifying the data subjects in case that their personal data are accessed or transferred to third parties, and obligations related to the creation of transparency logs, e.g., [40].

- **Technical security:** The XACML access control engine can enforce that the personal data that is disclosed can only be accessed according to the agreed-upon sticky policy. As PPL is based on XACML, the sticky policies can be enforced together with other access control policies by the XACML access control engine.

7.5 Provenance, Reputation and PETs

The notional dissonance between privacy requirements and reputation systems can be partially addressed with PETs. PETs that are designed for reputation systems aim at preserving the privacy of data subjects and/or service providers. In the case of data subjects, PETs aim to prevent third parties to link multiple feedback reports to a data subject — the goal of the third party is to profile which services a data subject uses. In the case of service providers, assuming that a data subject offers a service to other peers, e.g., a carpooling or participatory sensing application, PETs preserve the data subjects privacy by preventing third parties to link reputation values to individuals. In addition, it is fundamental that PETs are designed to thwart attacks against reputation systems, such as *white-washing* [19] and Sybil attacks [14].

To prevent profiling based on recommendation reports, a privacy-enhancing reputation system using role pseudonyms is presented in [33].[5] The proposal is based on self-certified pseudonyms that are valid for a given context or service and it limits its users to have at most one pseudonym per service [1, 32], which prevents Sybil attacks and *white-washing*. In addition, pseudonyms issued for different services are cryptographically unlinkable. Reputation can be transferred between different pseudonyms belonging to a same user using different cloaking techniques, as shown in [9]. Another proposal with the same objective, but based on the homomorphic encryption of the recommendation reports, is described in [42]. It preserves the privacy of the users providing feedback by exchanging and aggregating recommendations under encryption. However, this proposal requires all participants to strictly follow its protocols and it is not robust against misbehaving users.

Privacy-preserving logging schemes can help to determine data provenance and protect users' privacy, such as the ex post TET described in Section 7.2.

[5] Role pseudonyms are pseudonyms that are limited to a specific role or context [37].

8 Summary and Open Challenges

In this chapter we discussed privacy in SCIS. SCIS is based on technical concepts such as profiling, provenance and reputation systems, which pose privacy risks, as these techniques allow to track and analyze the users' habits and lifestyle. On the other hand, we also discussed the inherent characteristics of SCIS that can be utilized for a privacy-enhanced system design. While we have pointed out how legal means and PETs can help to protect privacy, still several challenges remain.

Technical challenges to be addressed for promoting privacy-enhanced SCIS in future include: composing peer profiles in a privacy-preserving manner and enforcing privacy-enhancing identity management for audience segregation of peers, utilization of the distributed nature of SCIS for building-in privacy, and combing privacy-preserving logging schemes with data provenance schemes.

References

1. Andersson, C., Kohlweiss, M., Martucci, L.A., Panchenko, A.: A Self-Certified and Sybil-Free Framework for Secure Digital Identity Domain Buildup. In: Information Security Theory and Practices: Smart Devices, Convergence and Next Generation Networks, Proceedings of the 2^{nd} IFIP WG 11.2 International Workshop (WISTP 2008), Lecture Notes in Computer Science, LNCS 5019, pp. 64–77. Springer (2008)
2. Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E.: Towards Usable Privacy Policy Display & Management for PrimeLife. Information Management & Computer Security **20**(1), 4–17 (2012)
3. Art. 29 Data Protection Working Party: Advise paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. Available at `http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf` (13.05.2013)
4. Bonabeau, E.: Decisions 2.0: the power of collective intelligence. MIT Sloan management review **50**(2), 45–52 (2009)
5. Buchegger, S., Crowcroft, J., Krishnamurthy, B., Strufe, T.: Decentralized Systems for Privacy Preservation (Dagstuhl Seminar 13062). Dagstuhl Reports **3**(2), 22–44 (2013). DOI http://dx.doi.org/10.4230/DagRep.3.2.22. URL `http://drops.dagstuhl.de/opus/volltexte/2013/4017`
6. Buchegger, S., Schiöberg, D., Vu, L.H., Datta, A.: PeerSoN: P2P social networking - early experiences and insights. In: Proceedings of the 2^{nd} ACM Workshop on Social Network Systems Social Network Systems 2009, co-located with Eurosys 2009, pp. 46–52. Nürnberg, Germany (2009)
7. Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.): Privacy and Identity Management for Life. Springer (2011)
8. Camenisch, J., van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9^{th} ACM conference on Computer and communications security, pp. 21 – 30 (2002)
9. Christin, D., Roßkopf, C., Hollick, M., Martucci, L.A., Kanhere, S.S.: Incognisense: An anonymity-preserving reputation framework for participatory sensing applications. Pervasive and Mobile Computing **9**(3), 353–371 (2013)
10. Council of Europe: Recommendation cm/rec(2010)13 of the committee of ministers to member states on the protection of individuals with regard to automatic processing of personal data

in the context of profiling. Available at https://wcd.coe.int/ViewDoc.jsp?id=1710949 (2010)
11. Cutillo, L.A., Molva, R., Strufe, T.: Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network. In: WOWMOM, pp. 1–6. IEEE (2009)
12. Dellarocas, C.: Online reputation systems: How to design one that does what you need. Sloan Management Review **51 (3)**, 33–38 (2010)
13. Dingledine, R., Mathewson, N., Syverson, P.F.: Tor: The second-generation onion router. In: USENIX Security Symposium, pp. 303–320. USENIX (2004)
14. Douceur, J.R.: The Sybil Attack. In: P. Druschel, F. Kaashoek, A. Rowstron (eds.) Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS), vol. 2429, pp. 251–260. Springer-Verlag (2002)
15. Dwork, C.: Differential privacy: A survey of results. In: M. Agrawal, D.Z. Du, Z. Duan, A. Li (eds.) TAMC, *Lecture Notes in Computer Science*, vol. 4978, pp. 1–19. Springer (2008)
16. European Commission: Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 C7 0025/2012 2012/0011(COD)) Compromise amendments on Articles 1-29. Available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf (21.10.2013)
17. European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (23.11.1995)
18. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final 2012/0011 (COD). Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (25.1.2012)
19. Feldman, M., Chuang, J.: Overcoming free-riding behavior in peer-to-peer systems. SIGecom Exch. **5**(4), 41–50 (2005)
20. Fischer-Hübner, S.: IT-Security and Privacy – Design and Use of Privacy-Enhancing Security Mechanisms, *Lecture Notes in Computer Science*, vol. 1958. Springer-Verlag Berlin/Heidelberg (2001)
21. Friedman, A., Schuster, A.: Data mining with differential privacy. In: B. Rao, B. Krishnapuram, A. Tomkins, Q. Yang (eds.) KDD, pp. 493–502. ACM (2010)
22. Gedik, B., Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Trans. Mob. Comput. **7**(1), 1–18 (2008)
23. Giunchiglia, F., Maltese, V., Anderson, S., Miorandi, D.: Towards hybrid and diversity-aware collective adaptive systems (2013)
24. Goffman, E.: The presentation of self in everyday life. Doubleday Anchor Books. Doubleday (1959)
25. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: Proceedings of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys 2003), pp. 31–42. USENIX (2003)
26. Hedbom, H., Pulls, T., Hjärtquist, P., Lavén, A.: Adding secure transparency logging to the prime core. In: M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, G. Zhang (eds.) The Future of Identity in the Information Society, Proceedings of the 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, vol. 320, pp. 299–314. Springer Berlin Heidelberg (2009)
27. Hildebrandt, M.: FIDIS Deliverable D7.12: Behavioural biometric profiling and transparency enhancing tools. Available at http://www.fidis.net/resources/fidis-deliverables/profiling/#c2369 (2009)
28. Kosinski, M., Stillwell, D., Graepel, T.: Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences **110**(15), 5802–5805 (2013)

29. Li, N., Li, T., Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity. In: R. Chirkova, A. Dogac, M.T. Özsu, T.K. Sellis (eds.) ICDE, pp. 106–115. IEEE (2007)
30. Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: *L*-diversity: Privacy beyond *k*-anonymity. TKDD **1**(1) (2007)
31. Martucci, L.A., Andersson, C., Fischer-Hübner, S.: Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks. In: Proceedings of the 1^{st} International Workshop on Security (IWSEC 2006), pp. 123–134. Information Processing Society of Japan (IPSJ) (2006)
32. Martucci, L.A., Kohlweiss, M., Andersson, C., Panchenko, A.: Self-Certified Sybil-Free Pseudonyms. In: Proceedings of the 1^{st} ACM Conference on Wireless Network Security (WiSec'08), pp. 154–159. ACM Press (2008)
33. Martucci, L.A., Ries, S., Mühlhäuser, M.: Sybil-Free Pseudonyms, Privacy and Trust: Identity Management in the Internet of Services. Journal of Information Processing **19**, 317–331 (2011)
34. Merriam-Webster.com: Profile. Available at `http://www.m-w.com/dictionary/profile` (2013)
35. Narayanan, A., Shmatikov, V.: De-anonymizing social networks. In: Security and Privacy, 2009 30th IEEE Symposium on, pp. 173–187. IEEE (2009)
36. Organisation for Economic Cooperation and Development (OECD): Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)
37. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Available at `http://dud.inf.tu-dresden.de/literatur/Anon\_Terminology\_v0.34.pdf` (2010). V0.34
38. PrimeLife: PrimeLife – Privacy and Identity Management in Europe for Life: Policy Languages. Available at `http://primelife.ercim.eu/images/stories/primer/policylanguage-plb.pdf` (2011)
39. Pulls, T.: Privacy-Preserving Transparency-Enhancing Tools. Licentiate Thesis, Karlstad University, 2012:57 (2012)
40. Pulls, T., Peeters, R., Wouters, K.: Distributed Privacy-Preserving Transparency Logging. In: Proceedings of the 12^{th} annual ACM Workshop on Privacy in the Electronic Society, WPES 2013, Berlin, Germany. ACM (2013)
41. Reiter, M.K., Rubin, A.D.: Crowds: anonymity for web transactions. ACM Transactions on Information and System Security (TISSEC) **1**(1), 66–92 (1998). DOI http://doi.acm.org/10.1145/290163.290168
42. Ries, S., Fischlin, M., Martucci, L.A., Mühlhäuser, M.: Learning whom to trust in a privacy-friendly way. In: Proceedings of the 10^{th} International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011), pp. 214–225. IEEE Computer Society (2011). DOI 10.1109/TrustCom.2011.30
43. Sweeney, L.: *k*-Anonymity: a Model for Protecting Privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems **10**(5), 557–570 (2002)
44. W3C: Platform for privacy preferences (P3P) project. Available at `http://www.w3.org/P3P/` (2006)
45. Warren, S., Brandeis, L.: The Right to Privacy. Harvard Law Review **4**(5) (1890)
46. Wästlund, E., Fischer-Hübner, S.: PrimeLife Deliverable D4.2.2: End user transparency tools: UI prototypes. Available at `http://primelife.ercim.eu/` (2010)
47. Westin, A.F.: Privacy and Freedom. Atheneum, New York, NY, USA (1967)