Enhancing privacy protection in social network systems through decentralization and policy conflict management

Regina Paiva Melo Paiva Melo Marin

CentraleSupélec

N° d'ordre : 2015-20-TH

CentraleSupélec

École Doctorale MATISSE

Mathématiques, Télécommunications, Informatique, Signal, Systèmes Électroniques

Laboratoire IRISA

THÈSE DE DOCTORAT

DOMAINE : STIC

Spécialité : Informatique

Soutenue le 7 septembre 2015

par :

Regina PAIVA MELO MARIN

préparée dans l'équipe de recherche CIDRE
Confidentialité, Integrité, Disponibilité, Répartition
CentraleSupélec / Inria

Enhancing Privacy Protection in Social Network Systems Through Decentralization and Policy Conflict Management

Composition du jury

Directeur de thèse :	Christophe BIDAN	Professeur, CentraleSupélec, France
Co-directeur de thèse :	Guillaume PIOLLE	Professeur assistant, CentraleSupélec, France
Président du jury :	Gildas AVOINE	Professeur, INSA Rennes, France
Rapporteurs :	Daniel LE MÉTAYER	Directeur de Recherche, INRIA Grenoble Rhône -Alpes, France
	Benjamin NGUYEN	Professeur, INSA Centre Val de Loire, France
Examinateurs :	Philippe JAILLON	Ingénieur de Recherche, École des Mines de Saint -Étienne, France

I dedicate this thesis to my love Luciano.

"Follow your bliss. If you do follow your bliss, you put yourself on a kind of track that has been there all the while waiting for you, and the life you ought to be living is the one you are living. When you can see that, you begin to meet people who are in the field of your bliss, and they open the doors to you. I say, follow your bliss and don't be afraid, and doors will open where you didn't know they were going to be. If you follow your bliss, doors will open for you that wouldn't have opened for anyone else."

Joseph Campbell

Acknowledgements

First of all, I would like to express my gratitude to my advisors, Dr. Christophe Bidan and Dr. Guillaume Piolle. They were always available to guide and advise me during the doctoral period. Thank you very much for all the technical support, as well as the opportunity to working and sharing experiences in the CIDre team.

Also, I would like to thank all the members of the CIDre team for all the interesting discussions we had during these years.

I would like to thank the reviewers, Drs. Daniel Le Métayer and Benjamin Nguyen. They expended an important time reading and suggesting corrections about this thesis. I would like to extend my gratitude to Drs. Gildas Avoine and Philippe Jaillon to accept the invitation to be in the jury of this thesis.

I would like to thank my mother Heloisa, my father Romualdo (*in memoriam*), my brothers Helton, Eugenio, and my nieces Sofia and Rafaella. Also, I extend my gratitude to my parents-in-law: Berenice, Heitor and Gustavo. Be writing these acknowledgements just became possible because they have been supporting me during important periods of my life. I would like to extend these acknowledgements to all my relatives, specially: Madrinha Nazaré, Tia Tête, Madrinha Socorrinha, Tia Mota, Madrinha Fransquinha, Solange, Ana Maria, Rosa, and Fatima.

Special thanks to my dear friends: Heverson, André, Stefanie, Erwann, Annie, Carmen, Remi, Ricardo, Florina, Bosco, Janaina, Veronique, Kate and Eunice. They always helped me, shared their time, ideas, experiences and knowledge.

Finally, I would like to thank my husband, Luciano. Your force, courage and companionship are my infinite inspiration. Thank you for your true love.

Regina Paiva Melo Marin
Rennes, September 2015.

Contents

Résumé en français **17**

Introduction **23**

I State of the Art **29**

1 Privacy Protection **31**
1.1 Types of Privacy Violations . . . 32
1.2 Personal Data . . . 35
1.3 Standards . . . 36
1.3.1 OECD Guidelines . . . 36
1.3.2 Canadian Standards Association Model Code - CSAC . . . 37
1.3.3 European Data Protection Directive 95/46/EC . . . 38
1.3.4 Comparative Analysis . . . 40
1.4 Digital Privacy Attacks . . . 41
1.4.1 Tracking . . . 41
1.4.2 Profiling . . . 43
1.4.3 Identity Theft . . . 43
1.5 Privacy Enhancing Technologies . . . 44
1.5.1 Protection of User's Identity in Email Systems . . . 44
1.5.2 Protection of User's Identity when Accessing Interactive Systems . . . 45
1.5.3 Protection of Users' Data . . . 46
1.5.4 Anonymous Credentials . . . 46
1.5.5 Privacy Policy Management . . . 47
1.5.6 Privacy in Databases . . . 48
1.6 Privacy by Design . . . 49
1.7 Conclusion . . . 51

2 Social Network Systems **53**
2.1 History and Evolution of SNSs . . . 54
2.2 Overview of SNSs . . . 55
2.2.1 Basic Elements of SNSs . . . 55

2.2.2 Usage Profile Categorization . . . 57
2.2.3 Functionalities of SNSs . . . 59
2.3 Centralized SNSs . . . 60
2.3.1 Discussion about Centralized SNSs . . . 62
2.4 Decentralized SNSs . . . 63
2.4.1 Networks of Trusted Servers . . . 64
2.4.2 Peer-to-Peer (P2P) Systems . . . 65
2.4.3 Hybrid Systems . . . 67
2.4.4 Discussion about Decentralized SNSs . . . 68
2.5 Conclusion . . . 69

3 Privacy in SNSs 71
3.1 Privacy Issues in SNSs . . . 71
3.1.1 Malicious Authenticated User . . . 72
3.1.2 Malicious Third-party Application Providers . . . 73
3.1.3 Malicious Authoritative Entity . . . 74
3.1.4 Privacy-enhanced SNSs . . . 74
3.2 Privacy Policy Management . . . 76
3.2.1 Privacy Settings in Existing SNSs . . . 76
3.2.2 Access Control Policies and Privacy Policies . . . 78
3.2.3 Privacy Policy Languages . . . 80
3.2.4 User Privacy Policy vs. Service Provider Privacy Policy . . . 83
3.2.5 Policy Conflicts . . . 86
3.2.6 Policy Management Architecture . . . 87
3.3 Privacy Regulations for SNSs . . . 88
3.4 Conclusion . . . 89

II Enhancing Privacy Protection in SNSs 91

4 An Analysis Grid for Privacy-related Properties of Social Network Systems 93
4.1 Similar Research Works . . . 94
4.2 Degrees of Decentralization . . . 95
4.3 Privacy-related Properties for SNSs . . . 96
4.3.1 Architectural Services . . . 96
4.3.2 Storage . . . 98
4.3.3 Privacy Policy Management . . . 99
4.3.4 Security Aspects of Privacy . . . 101
4.4 The Multi-criteria Analysis Grid . . . 103
4.4.1 Facebook . . . 104
4.4.2 Safebook . . . 106
4.4.3 SuperNova . . . 107
4.4.4 Diaspora . . . 108
4.4.5 PrivacyWatch . . . 108

4.4.6 PeerSoN . . . 110
4.4.7 FOAF . . . 110
4.5 Interpretation in a Lattice Structure . . . 111
4.6 Making Recommendations to Developers . . . 113
4.6.1 Composition of Properties . . . 114
4.7 Limitations of the Contribution . . . 119
4.8 Conclusion . . . 119

5 Equity-preserving Management of Privacy Policy Conflicts in SNSs 123
5.1 Privacy Conflicts in SNSs . . . 124
5.1.1 Data Sharing in SNSs . . . 124
5.1.2 Information Sharing Architecture . . . 125
5.1.3 Expressing Privacy Policies in SNSs . . . 127
5.1.4 Conflict Resolution Strategies . . . 128
5.2 Equity Approach to Conflict Management . . . 129
5.2.1 The Notion of Equity . . . 129
5.2.2 An Equity-preserving Conflict Management Algorithm . . . 131
5.3 Consent . . . 135
5.4 Related Works . . . 137
5.5 Limitations . . . 137
5.6 Conclusion . . . 138

6 Implementation and Evaluation of Equity-preserving Management in SNSs 141
6.1 Measuring Equity . . . 141
6.2 Prototype Implementation . . . 144
6.3 The Experimental Setup . . . 146
6.3.1 Fictitious SNS Experiment . . . 146
6.3.2 Facebook SNS Experiment . . . 148
6.4 Discussion . . . 149
6.4.1 Limitations of the Implementation . . . 149
6.4.2 Impact of Design Choices . . . 150
6.5 Conclusion . . . 151

Conclusions and future works 153

A Publications and Research Activities 155

Bibliography 157

List of Figures

1.1 Solove's taxonomy of privacy violations 33

2.1 Timeline of the main SNSs since 1997 (adapted from Boyd and Ellison [BE07]) 56
2.2 Functionalities of SNSs 60
2.3 Safebook's architecture 66
2.4 PrivacyWatch's architecture 68

3.1 Policy management architecture 88

4.1 Types of communication networks [Bar64] 95
4.2 Privacy-related properties for SNSs 97
4.3 Lattice based on the data encryption (A) and traffic communication encryption (B) properties 112

5.1 The SNS scenario specification 125
5.2 Information sharing architecture 126
5.3 The equity-preserving conflict management algorithm 132

6.1 Graphical representation of the Gini coefficient 142
6.2 Graphical representation of the Gini coefficient 143
6.3 Implementation of equity-preserving algorithm 145
6.4 Strategy results in a very unbalanced population 147
6.5 The strategies' outcomes using the Facebook population 149

List of Tables

1.1 Similarities among principles 42
1.2 Solove's taxonomy and PETs mapping 50

2.1 Dominant SNSs according to the continent and the region 59

3.1 Privacy policy elements in SNSs 80
3.2 Administrative policy features in SNSs 86

4.1 Minimal number of entities to be compromised depending on the attacker model 100
4.2 The multi-criteria analysis grid applied at SNSs proposals 105
4.3 Composition of properties 120

Résumé en français

Améliorer la protection de la vie privée dans les systèmes de réseaux sociaux par la décentralisation et la gestion des conflits de politiques

Présentation

Cette thèse se place dans le contexte de la protection de la vie privée dans les applications de réseaux sociaux en ligne, en particulier par une démarche de décentralisation des services et des contenus. Elle est articulée autour de deux contributions techniques qui répondent à des problématiques identifiées :

- Une grille d'analyse, associée à des outils formels, permet d'évaluer précisément le niveau de protection de vie privée assuré par une plate-forme, en analysant le niveau de décentralisation de seize propriétés techniques ;
- Un nouvel algorithme de résolution de conflits, correctement intégré dans un système de réseau social distribué, permet d'arbitrer les conflits entre des politiques de sécurité incompatibles tout en assurant une certaine équité entre les différents participants, du point de vue du respect de leur politique.

Contexte et état de l'art

Protection de la vie privée

Le droit à la vie privée, associé à sa nécessaire protection, est un concept qui a émergé au cours du XX^{e} siècle dans les sociétés démocratiques. Il s'agit d'une notion complexe et partiellement subjective, en interaction avec d'autres droits et d'autres concepts. L'accroissement significatif des moyens de traitement informatique puis, plus tard, l'avènement d'Internet et l'évolution de ses usages, ont eu un impact significatif sur l'importance de la notion de vie privée, sur les risques associés et sur leur perception par le public.

Des brèches de vie privée surviennent lorsque des informations personnelles sont collectées, traitées ou disséminées de manière inappropriée ou non autorisée. Cela peut avoir diverses conséquences pour la victime, qu'il s'agisse d'embarras, de détresse psychologique,

d'atteintes à sa réputation ou encore de dommages financiers. Les mesures prises pour prévenir ces brèches et limiter leur impact sont principalement de deux ordres, juridique et technique. Du point de vue juridique, de nombreux pays ont introduit un cadre spécific de protection des données personnelles, régulant la collecte, la conservation, l'utilisation et la communication d'informations relatives à des personnes physiques. C'est notamment le cas de l'Union européenne, avec la directive 95/46/EC et le projet de réglement européen chargé de la remplacer. Du point de vue technique, de nombreux outils et méthodes spécifiques de protection sont regroupés sous le terme de PETs (*Privacy Enhancing Technologies*, technologies améliorant la vie privée). Ces outils sont généralement focalisés sur la protection d'une propriété de sécurité particulière, dans un type de scénario donné. La protection de la vie privée par conception, ou *Privacy by Design*, est quant à elle une démarche intégrée visant à s'assurer que les propriétés de protection de la vie privée des personnes sont prises en compte à chaque étape du cycle de vie d'un produit ou d'un service, et par tous les acteurs.

Le cas particulier des réseaux sociaux

Le besoin de protéger la vie privée des individus par des outils spécifiques est particulièrement fort dans le cadre du web, dans lequel les utilisateurs finaux sont de plus en plus impliqués dans la création et la publication de contenu. Assez significativement, les Systèmes de Réseaux Sociaux (SRS) y sont actuellement le type d'application le plus utilisé. Ils sont de natures, de vocations et de fonctionnalités variées. Leur point commun est d'être des plates-formes en ligne permettant aux individus de reproduire sur Internet des interactions sociales comparables à celles du monde physique, et d'accéder à des personnes, des contenus et des informations au travers de ce réseau d'interactions. Si la sémantique de ce graphe social diffère souvent d'un SRS à un autre, les utilisateurs y publient souvent un "profil" généralement constitué d'informations personnelles comme des photographies, des vidéos, des informations relatives à leur identité, à leurs activités, à leurs préférences...

Les SRS posent des problèmes de vie privée spécifiques, à cause de leur objet même, qui consiste à faciliter la publication et l'accès à des contenus liés à des individus. Des risques de brèches de vie privée existent au niveau du fournisseur de service, des utilisateurs finaux et des fournisseurs d'applications tierces. En particulier, le profilage comportemental des utilisateurs est un risque particulièrement prégnant dans les SRS, qui concentrent toutes les informations nécessaires à cette fin. Les risques en matière de vie privée dépendent toutefois des choix architecturaux et techniques opérés par les concepteurs de ces systèmes. En particulier, l'immense majorité des SRS sont développés autour d'une architecture centralisée et donnent au fournisseur de service un pouvoir significatif sur les données qui lui sont confiées, augmentant ainsi les risques d'abus.

De nombreuses propositions techniques existent pour concevoir des SRS décentralisés afin de limiter les risques liés à l'existence d'une autorité unique. À quelques exceptions près ces plates-formes demeurent des démonstrateurs de recherche. On constate que la classification usuelle en "centralisé", "décentralisé" et "distribué" échoue à capturer les différences de choix architecturaux entre ces propositions, mettant ainsi en lumière le besoin d'une meilleure méthodologie d'analyse pour évaluer leur impact sur la vie privée.

Contributions

Une grille d'analyse détaillée de la protection de la vie privée dans les systèmes de réseaux sociaux

Lorsqu'on examine les propositions techniques de SRS décentralisés, il apparaît que la centralisation ou la décentralisation n'est pas un concept monolithique et que des choix techniques différents sur des points de détail peuvent avoir un impact significatif sur divers aspects de la vie privée.

Afin d'évaluer finement l'influence des choix de conception sur la protection des utilisateurs, seize propriétés techniques ont été identifiées et réparties dans quatre catégories :

- Services architecturaux (recherche, récupération, communication) ;
- Stockage (espace de stockage, réplication, suppression) ;
- Gestion des politiques de vie privée (administration et mise en œuvre des politiques système et des politiques des utilisateurs) ;
- Aspects de la vie privée liés à la sécurité (chiffrement des données, chiffrement du trafic, anonymat, pseudonymat, non-chaînabilité et non-observabilité).

Il a été défini clairement ce que signifiait, pour chacune de ces seize propriétés, d'être "centralisée", "décentralisée" ou "distribuée". En particulier, pour la dernière catégorie, il a été nécessaire de s'appuyer sur la définition de modèles d'attaquants spécifiques, déterminés à violer une propriété donnée pour l'ensemble des utilisateurs du système et voyant leurs capacités dépendre du niveau de décentralisation.

Le résultat de cette étude est une grille d'analyse détaillée, associée à une structure en treillis permettant de comparer de diverses manières les SRS considérés. À titre d'exemple, l'analyse de six systèmes décentralisés (SuperNova, Diaspora, PrivacyWatch, PeerSon, Safebook et FOAF) est fournie en regard de celle de Facebook. Cette grille d'analyse peut également être vue comme un outil de protection de la vie privée par conception. Son étude a notamment permis la formulation de recommandations techniques détaillées, destinées à des concepteurs de SRS et portant sur des combinaisons de propriétés techniques particulières comportant des avantages précis en matière de vie privée ou permettant une amélioration significative du niveau de protection par rapport à des choix plus classiques.

Gestion des conflits de politiques de vie privée préservant l'équité

Les SRS, comme nombre d'autres applications, donnent aux utilisateurs le contrôle de leurs information par le biais de politiques de vie privée, un type de politiques de sécurité spécialement adapté aux problématique de partage d'informations personnelles. Il existe de nombreux formalismes pour cela, souvent dérivés de langages de contrôle d'accès et plus ou moins adaptés aux spécificités de la protection des données personnelles.

Par le biais de ces politiques, un utilisateur peut par exemple spécifier qui peut accéder ou pas à une photographie qu'il met à disposition. Néanmoins, si l'objectif est de protéger la vie

privée et non la paternité sur un document, les autres personnes figurant éventuellement sur cette photographie devraient également pouvoir émettre une telle politique : fournir ce type de contrôle aux sujets des données, et non simplement à leur possesseur ou à leur créateur, est un objectif qui devrait être poursuivi par tout SRS visant à améliorer la protection de la vie privée. Il en résulte que lorsqu'un utilisateur demande à accéder à une photographie, il faut considérer plusieurs politiques de sécurité différentes avant d'accorder ou pas l'accès. Il peut arriver que ces politiques soient incompatibles entre elles, certaines accordant l'accès et d'autres le refusant.

Ces conflits entre politiques sont un problème d'autant plus présent dans les applications distribuées. Ils sont gérés de manières diverses par les SRS et les autres types de systèmes d'information, la stratégie la plus répandue consistant à refuser l'accès dès lors qu'au moins un participant le requiert. Il s'avère que toutes ces stratégies peuvent potentiellement mener à des situations inéquitables, dans lesquelles certains utilisateurs voient leur politique moins souvent respectée que les autres. Une définition de l'équité d'une situation dans un SRS a été proposée en ce sens, ainsi qu'un algorithme de résolution de conflit visant à améliorer cette équité, en tendant à favoriser les individus qui ont vu leur politique violée plus fréquemment lors des interactions passées.

Cet algorithme, ainsi que ceux correspondant aux stratégies classiques, a été mis en œuvre au sein d'un démonstrateur logiciel. Ce programme a été utilisé pour simuler des interactions de partage de photographies dans un SRS de quatre mille utilisateurs, organisés suivant une topologie extraite du réseau Facebook. Les résultats obtenus avec les différentes stratégies de résolution de conflits ont été enregistrées sur des séries de quarante mille interactions. Le coefficient de Gini a été utilisé pour mesurer l'impact du choix de la stratégie sur l'équité globale du système. Il s'agit d'un indicateur, compris entre 0 et 1, largement utilisé en économie pour mesurer les inéquités dans la répartition d'une richesse sur une population. Il a ici été appliqué à la répartition de la proportion de violation des politiques sur la population des utilisateurs. Il a pu être observé que l'algorithme proposé donnait de bien meilleurs résultats que les autres, affichant un Gini meilleur de 0.2 par rapport à la deuxième meilleure stratégie. Cette différence significative correspond à la différence d'équité dans la répartition des revenus 2005 entre la Suède et l'Iran.

Des recommandations ont également été formulées sur l'intégration correcte d'un tel algorithme dans un SRS, de manière qu'une décision d'arbitrage automatisée ne viole pas le consentement des utilisateurs. Deux options sont proposées pour cela, l'une consistant à proposer aux utilisateurs de concéder des exceptions ponctuelles à leur politique, la deuxième à leur suggérer de modifier durablement certaines règles de leur politique pour limiter l'apparition d'inéquités.

Conclusion

Ces travaux de recherche ont débouché sur deux contributions significatives, susceptibles d'améliorer la maniére dont la protection de la vie privée est prise en compte dans les systèmes de réseaux sociaux, et plus spécifiquement dans le cadre d'une décentralisation de ces applications.

Ils ouvrent également de nouveaux axes de recherche, orientés notamment vers l'approfondissement et l'amélioration des contributions présentées. En particulier, l'impact de choix de conception détaillées d'un SRS décentralisé (issus de la grille d'analyse) sur la mise en œuvre technique de l'algorithme proposé pour l'arbitrage des conflits reste à évaluer de manière systématique. Des risques de manipulation de l'algorithme d'arbitrage par des utilisateurs malveillants sont également identifiés et nécessitent une attention particulière. De plus, des pistes techniques sont proposées pour distribuer efficacement le processus d'arbitrage, l'absence de point de décision centralisé restant accepté par la communauté scientifique comme un critère essentiel pour la protection de la vie privée.

Introduction

Context

Social Network Systems (SNSs) are the predominant web service around the world. They attract many users seeking popularity, entertainment and network social building, along with ease of use. Users publish, redistribute and generate detailed contents about themselves such as photos, music, hobbies, etc. Moreover, SNSs allow users to easily share data and link them to other users.

The increasing acceptance of SNSs is due to the fact that they contribute to fill the societal need to communicate and exchange messages and information with others through several available activities that attempt to reproduce many aspects of a person's social life. As a consequence of the range of interactions within the SNS, sites like Facebook, Twitter and LinkedIn gather a massive amount and diversity of personal information such as name, address details, interests, educational information or professional experiences, amongst others.

In current SNSs, the information of all users is aggregated in a centralized storage which is under the control of a single SNS provider (also called central authoritative entity). The SNS provider retains full control of all users' personal data [BKW09, CMS09, GKB12]. It can access all data in the system including private messages and browsing behavior. For this reason, the centralized architecture of existing SNSs is prone to privacy violations of users' data, especially by the SNS provider, which can perform several analysis and leakage to third parties. To overcome the issues raised by centralized control, different approaches have been proposed towards the decentralization of data and services. Decentralization transfers control and services from the SNS provider to users, allowing them to enable privacy protection over personal data.

An important step towards the protection of privacy in centralized or decentralized architectures is the use of privacy policies. When users subscribe to an SNS in order to join the system, policies provide them with setting options for preserving data privacy. Privacy policies require to set the visibility and the accessibility of data to others, granting privileges to different entities (e.g., user's friends, friends of friends, all users).

In the SNS context, users often have rich and complex privacy policies [SHC+09, BKS+09]. Users can post information on their profiles and upload content such as pictures and videos. The user that publishes information on her webspace is able to specify policies, regulating the people with whom the information can be shared. However, in many circumstances the document that is released in the user's webspace often conveys information that is not related

only to her profile. For instance, a user is able to upload a group picture without consulting the privacy preferences of other users appearing in the photo, even if they are identified by tags.

Motivations

The development of most SNSs are based on centralized designs, which are less likely to improve privacy since there is a single and central authority with exclusive administration control over users' information. Many proposals have been introduced that work towards decentralizing the infrastructure support in order to enhance privacy in SNSs. Generally, the more decentralized the SNS, the better the privacy protection, which can happen in different degrees. However, designing decentralized SNSs driven by privacy protection is a hard task because privacy is impacted by most design choices. These design options are used to build SNSs in which data remain with users. These efforts to protect users' data are useful, but there are many challenges when shifting the concept from centralized to decentralized architecture. Nonetheless, it is not clear how to design decentralized SNSs that achieve good balance among privacy protection on the one hand, and availability, usability, and performance on the other hand.

While decentralization solves issues involving the SNS provider, privacy policies play a leading role in the protection of unauthorized data access from other users when sharing information. In environments such as SNSs, human interactions and relationships potentially allow for the sharing of information with others. Typically, information that is shared among users may be subject to conflicting policies. Given the difficult to reach an agreement when a decision is based on the preferences of multiple users over a shared resource, most SNSs use a naïve approach in which the user who publishes the resource has the highest priority. The strategy provided by SNSs to manage shared content is a simplistic solution and may lead to unfair situations [SSP09], and according to data protection regulation, other users should be provided with rights to control the processing and disclosure of the documents relating to them [PtC95].

Problem Statement

The main goal of this thesis is to enhance the level of privacy in the context of SNSs. In addressing privacy issues, the first means to be considered is the decentralization of data. Traditional SNSs were not developed implementing privacy on the top application. If privacy is not considered at the early phase of the SNS development, it becomes very complicate for the developers to integrate privacy in later phases.

In recent years, different decentralized approaches have been proposed, aimed at enhancing privacy issues raised by centralized control. However, difficulties arise when designing a privacy-enhanced SNS driven by decentralization, which are not obvious for designers. Each decentralized SNS solution focuses on decentralizing some specific design points according to particular tradeoffs based on the designer's preferences and architectural choices. Methods to facilitate designers and engineering evaluation, comparison and classification of the existing

SNSs according to their core design of architectural choices are still a necessity. Such tool can guide designers to align design issues and distinguish best practices by the very beginning on the development of privacy-friendly SNS architectures.

In summary, the problem addressed is: **how to assess and compare SNSs with each other, according to the precise privacy-enhanced design choices on which they are based?**

As part of this thesis, a multi-criteria analysis grid has been proposed. This multi-criteria analysis grid allows to evaluate several properties related to privacy, and then classify SNSs with each others according to privacy properties. The contribution has been published at *The* 3^{rd} *Atelier sur la Protection de la Vie Privée (APVP 2012)* [PMMPB12] and *The* 5^{th} *ASE/IEEE International Conference on Social Computing (SocialCom 2013)* [MPB13].

Other privacy issues are related to the policy conflict management. For instance, let us consider a situation in which a user releases data in the SNS, but other users that are related to this data are able to define privacy policies for it. The management of the associated policies may lead to conflicts due to the multiplicity and heterogeneity of these privacy policies. Conflicts may arise when users privacy policies disagree about the allowed usages of a document, since every user has different privacy preferences. When the demands or desires of one part are in conflict with others, conflict resolution strategies generally try to achieve an effective resolution. However, a user can find that these strategies introduce unfair decision making, generating deceptive behaviour and violations of privacy rights.

For instance, let us consider three users (Alice, Bob and Charlie) interacting within the same SNS. Consider also a symmetric relation such that Alice is a friend of Bob, and Bob is a friend of Charlie. Alice uploads a document (e.g., a photo) on her webspace and tags Charlie in it. Suppose, on the one hand, that Alice authorizes only her friends to see the picture and, on the other hand, that Charlie has specified in his policy an interdiction, that nobody should be able to see the photos in which he appears. Bob wants to see a photograph shared by Alice and picturing Charlie, however Bob's access can be constrained by the policies of Charlie. If the "SNS strategy" is applied, the situation is somewhat unbalanced: Alice sees her preferences prevailing over others in the form of a more frequent enforcement of the policy; at the same time Charlie sees his preferences being violated. A systematic disparity can, on the long run, be considered unfair to other users since Charlie's privacy policy may never be enforced. Thus, due to the lack of a proper conflict strategy resolution, the fairness of such situations remains a largely unresolved issue for SNSs.

In summary, the problem addressed is: **how is it possible to enforce conflicting privacy policies without generating unfair situations?**

As part of this thesis, an equity-preserving conflict management algorithm has been proposed. This objective of the algorithm is to propose a fair strategy to resolve conflicts between SNSs users. The proposed algorithm has been evaluated using an appropriated metric. This contribution has been published at *The* 6^{th} *ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)* [MPB14].

Outline

This thesis is organized in two parts containing six chapters.

Part I comprises the state of the art, which is organized in three chapters. Chapter 1 provides the baselines on privacy protection, including an overview of regulatory and technological aspects of privacy and data protection. Chapter 2 presents perspectives on the development of SNSs, detailing basic elements and main functionalities based on their design and architecture. In chapter 3, privacy issues currently faced in SNSs are examined in deep and the motivation behind the need for improvement is explored.

Part II presents the contributions of this thesis, organized in three chapters. Chapter 4 introduces in details the development of the multi-criteria analysis grid designed to evaluate several properties of SNSs related to privacy. Based on the analysis grid result, privacy-related design choices are then organized in a lattice structure to classify and visualize SNSs in privacy-related hierarchies. Then, chapter 5 introduces the concept of equity in SNS in order to resolve conflicts of privacy policies and proposes an equity-preserving conflict management algorithm. Finally, chapter 6 describes the implementation and evaluates the efficiency of the equity-preserving conflict management algorithm (introduced in chapter 5) by using an appropriated metric, and presenting some experimental results.

The thesis is concluded with a summary of the developed methods and perspectives for future research.

Abbreviations

CSAC	Canadian standards association model code
DHT	Distributed hash table
E.U.	European union
EPAL	Enterprise privacy authorization language
FTC	Federal trade commission
FOAF	Friend-of-a-friend
GDPR	General data protection regulation
IT	Information technology
IP	Internet protocol
IBM	The international business machines corporation
NSA	National security agency
PbD	Privacy by design
NIST	National institute of standard and technology
OECD	Organization for economic cooperation and development
PETs	Privacy enhancing technologies
PGP	Pretty good privacy
P2P	Peer-to-peer
P3P	Platform for privacy preferences
PIPEDA	Personal information protection and electronic documents act
PII	Personally identifiable information
PSNS	Privacy-enhanced SNS
SNS	Social network system
SNSs	Social network systems
SSN	Social security number
SSL	Secure sockets layer
TLS	Transport layer security
TIS	Trusted identification system
U.S.	United state
UPP	User privacy policy
XACML	eXtensible access control markup language

Part I

State of the Art

Chapter 1

Privacy Protection

One of the most significant concepts in the contemporary democratic societies is privacy. Privacy is a multidimensional concept that encompasses different notions concerning personal information, freedom of intrusion, and protection from searches and surveillance.

Historically, a significant amount of work has been done on defining privacy. The original meaning of privacy came from the Latin word *privatus*: separated from the rest. In the Roman law, *privatus* provides the legal distinction between "private" and "public". Generally speaking, when a document has a stamp "private", only an authorized person with credentials has the right to access the information inside. From the Romans' notion of privacy and along the years, problems with individuals' private information is something that often occurs. From the 14^{th} throughout the 18^{th} century, people went to regional courts to complain about someone else's action of opening and reading their personal letters.

Since the end of the 19^{th} century, the emphasis shifted towards the control of individuals' own information [Hol09]. One of the most influential milestone in the history of privacy is the classical legal study *The Right to Privacy*, written by Warren and Brandeis in 1890 [WB90] in response to the possibility of intrusive press coverage taking instantaneous photography and publishing then without consent (i.e., a classical type of privacy invasion). They defined privacy as "*the right to be let alone*", with a focus on protecting an individual from interference of others.

The value of privacy is so relevant that is recognized as a basic human right in Article 12 of the United Nations' Universal Declaration of Human Rights [Ass48]:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack."

In 1967, a new turning point was reached with the publication of Alan Westin's book *Privacy and Freedom* [Wes67], defining privacy in terms of control against disclosure as the

"claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

In the last 50 years, due to the fast development of technology, privacy violations within the digital society has increased involving groups of people and nations. In 1971, the *Echelon Project* was formally established for military purposes during the Cold War, to monitor all international satellite telecommunications (e.g., phone calls, fax) from intelligence agencies in United State of America, United Kingdom, Canada, Australia and New Zealand. The *Carnivore Project*, implemented in 1997 by the Federal Bureau of Investigation (FBI) and publicly revealed in 2000, was a system that tracked the internet traffic communication by using custom packet sniffers [Hol09]. The latest public outcry is the *Prism Project*, the surveillance program operated since 2007 by the National Security Agency (NSA) and revealed by Edward Snowden in 2013. The Prism Project collects both non-encrypted and encrypted internet communications. Many important companies (Microsoft, Yahoo, Google, Facebook, Youtube, AOL, Skype and Apple) participated to it and provided users' personal information.

More recently, in 2006, privacy has been described by Günter Müller [Mül06] as *"the possibility to control the distribution and use of personal data"*, and is included into modern discussions regarding the control over how information flows in our online society [Boy10]. For Müller privacy is focused on how information is managed, while Westin views privacy as a mean to control information access. In spite of the existence of innumerable attempts to conceptualize privacy, still the debate continues without consensus.

Following Alan Westin's and Günter Müller's theories, in this thesis privacy is seen as a generalized but not absolute notion that focuses on the management of private information. In other words, to protect an individual's privacy, autonomy and control should be provided over private information with the ability to grant or deny access, collection, process and dissemination.

Although researchers and other professionals have been working to increase individuals' privacy, violations in people's activities and business still remain an important issue.

This chapter is dedicated to the field of privacy protection. Activities that may cause privacy violations are described in section 1.1. In section 1.2 types of data that should be protected to guarantee person's privacy are presented. Section 1.3 describes available standards for protecting privacy. In section 1.4 identifies three types of technology-based privacy problems. Section 1.5 describes Privacy-Enhancing Technologies as technical solutions to prevent unnecessary and/or undesired processing of personal data. Principles guiding the implementation of legal requirements into information systems solutions are depicted in section 1.6. Finally, some conclusions are presented in section 1.7.

1.1 Types of Privacy Violations

A privacy violation occurs when personal information is improperly or unauthorized collected, used, or disseminated. Often, when a privacy violations occur, victims are spoiled with embarrassment, mental distress, reputation problems, financial loss and other disadvantages.

An well-known classification of different types of privacy violations is given by the Solove's

taxonomy [Sol06]. It discusses privacy issues from a social-psychological perspective. This taxonomy well-recognized in the information privacy field and allowed Solove to win the 2006 Privacy Enhancing Technology award.

The taxonomy, made for an understanding of privacy in a pluralistic manner, consists in sixteen categories, classified in four principal groups of activities: information collection, information processing, information dissemination and invasion. Each group encompasses a diversity of activities that can lead to privacy violations. Figure 1.1 is a representation of Solove's taxonomy.

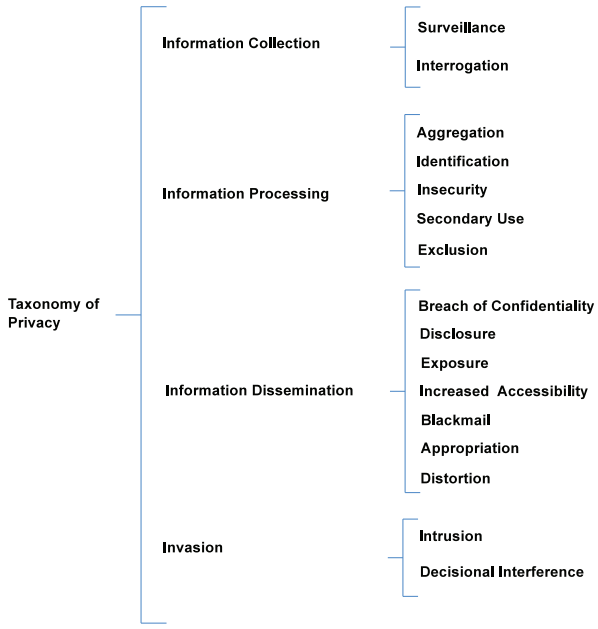

Figure 1.1 – Solove's taxonomy of privacy violations

The first group of activities is related to *information collection*. It affects privacy by making people worried about how the collected information could be used against them. There are two kinds of information collection: surveillance and interrogation. *Surveillance* is the observation of the subject's activities by watching, recording or listening in public or private places. *Interrogation* involves several forms of questioning, which may place people in a difficult position for answering intrusive questions about some subject (e.g., the U.S. state of Massachusetts prohibits employers to ask workers about personal imprisonment, or any about prior commitment to mental health treatment).

The second group of activities is *information processing*, which refers to how data is stored, used and manipulated after being collected. There are five kinds of violations related to information processing: aggregation, identification, insecurity, secondary use and exclusion. *Aggregation* consists in the combination of isolated pieces of information that can reveal unexpected facts about a person. *Identification* is the fact of linking a piece of information to an individual (through an identifier), allowing to reveal the identity of a person. *Insecurity* is the failure to protect stored information from leaks and improper access. *Secondary use*

occurs when the use of information differs from the original purpose, without the subject's consent. *Exclusion* is the failure to provide people information about their own records. Exclusion may violate legal processing and tends to reduce the accountability of organizations that maintain records.

The third group of activities is *information dissemination*. It involves the spreading or releasing of information to others. There are seven kinds of information dissemination: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion. *Breach of confidentiality* is the breaking of a promise to keep a person's information private. It involves the revelation of secrets about a person and violates the trust in a specific relationship (e.g., person's violation of confidential information provided by doctors, bankers, lawyers, and others). *Disclosure* involves the revelation of private and truthful information to unexpected parties, when the information is not of general public interest. *Exposure* involves dissemination to others of embarrassing information (physical and emotional) that affects a person's dignity, inducing feelings of vulnerability and distress (e.g., when a U.S. newspaper published a picture of a high school athlete whose genitalia were accidentally exposed while playing soccer[1]). *Increased accessibility* is the access amplification to a previously available information. *Blackmail* is the coercion of an individual by threatening to disclose personal information. *Appropriation* is the use of an individual's identity or personality by others for different purposes and goals. *Distortion* is the dissemination of false information about a person.

Finally, the fourth group of activities is *invasion*, which represents interference in people's lives. Solove describes two kinds of invasion: intrusion and decisional interference. *Intrusion* refers to incursions into one's life that disturbs one's tranquillity. It disturbs the victim's daily activities, alters routines, destroys solitude and the state of being alone. *Decisional interference* occurs when there is interference by an authority into the subject's decisions (e.g., the Supreme Court decided that is illegal for the government to forbid the use of contraceptives by married couples, U.S. 479, 485-86 (1965), in Griswold v. Connecticut).

These four groups of violations provide useful guidelines that help to visualize and analyze a wide variety of privacy problems. While Solove's types of violations exist independently of technology, they are primarily caused through activities of people, businesses, and by the government.

Solove's study attempts to analyze privacy violations in order to help policy makers to create policies and norms. The utility of the above four categories regarding social problems such as bodily integrity, freedom of expression, and invasion, is undeniable. Solove's criterion for inclusion in his taxonomic is that considered privacy problems must have been recognized by the society. On the other hand, Solove's taxonomy can be refined by introducing new types of digital privacy violations, which were not originally considered. The evolution of online services on the Internet, such as search engines and social networks, has lead to many modern challenges in terms of privacy. For instance, web tracking technologies are capable of following people's activities, interactions and contents and relating them to each other. Another relevant example is automated profiling, which builds profiles and may allow prediction (or discrimination) about people's behavior, attitude, and interests. It is important

[1] http://jour305.homestead.com/files/mcnamara.pdf

to note that these issues have different characteristics when compared to traditional privacy problems; they are the product of digital information flows, architectural design choices of systems and online social interactions. These kinds of violations, unknown to Solove, will be analyzed further later in this chapter.

Privacy violations lead to the conception and the application of data protection, which brings benefits to the management of information when properly applied.

1.2 Personal Data

Data protection is designed to protect individuals' privacy by regulating the conditions under which data can be collected, processed and disseminated. In the U.S. privacy laws, the term Personally Identifiable Information (PII) is used. The National Institute of Standard and Technology (NIST) Special Publication 800-122 [NIS09] (Guide to Protecting the Confidentiality of Personally Identifiable Information) defines PII as "*any information which can be used to distinguish or trace an individual's identity, such as name, social security number (SSN), date and place of birth, mother's maiden name, or biometric records; or when combined with other personal information which is linked or linkable to an individual, such as medical, educational, financial, and employment information*". The concept of PII intends to cover data that can directly identify an individual or make an individual identifiable.

European regulations take another approach to the issue. In the European Union (E.U.) Data Protection Directive, the term Personal Data is used. Personal Data, under the Directive 95/46/EC [PtC95] in article 2a, refers to "*any information relating to an identified or at least identifiable person, where an identifiable person is the 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, physiological, mental, economic, cultural or social identity*". Examples of personal data that can be identified are: full name, residential address, SSN, email address, Internet Protocol (IP) address, user's profiles in social networks, geolocated data, amongst others.

A special category of personal data that may pose a greater risk when processed, listed in the Directive 95/46/EC, is called *Sensitive Data* [PtC95]: personal data that reveals ethnic or racial origin, political opinion, religious or other similar beliefs, physical or mental health details or sexual life.

Nowadays, it is difficult to distinguish between personal and non-personal data because every form of interaction creates a certain amount of traces and almost every piece of data is related to a person somehow. Consequently, information appearing to be non-identifiable can be turned into identifiable data [SS11], and thus be used to identify an individual. For instance, in 2006, Netflix, the world's largest on-demand Internet streaming media company, released an anonymized database containing movie ratings in the context of the Netflix Prize competition, in order to improve their recommendation service. In few weeks, Narayanan and Shmatikov [NS08] identified the anonymized Netflix records of an individual by cross-referencing it with available records (such as the Internet Movie Database (IMDb)), based on the dates and titles of movie reviews.

In this thesis, the notion of Personal Data is adopted, rather than PII, since it encompasses

of all types of data that relate to an individual, in an direct or indirect manner (i.e., when combined or cross-checked with other information).

1.3 Standards

Due to different types of privacy violations, the necessity of a legal protection has become an important issue, and indeed many countries are seeking to protect privacy through constitutional laws, regulations and court examinations. Also, privacy regulations are growing in relevance and dictates how organizations and enterprises may collect, use, disclose, retain, and destruct personal information. Although the regulation and implementation of data protection vary across the globe, three standards have influenced modern worldwide privacy laws: the Organization for Economic Co-operation and Development (OECD), the Canadian Standards Association Model Code, and the European Data Protection Directive 95/46/EC.

1.3.1 OECD Guidelines

In 1980, the *Organization for Economic Co-operation and Development* (OECD) adopted principles for protecting personal data, including how data would be protected in cross border transactions among OECD members [OEC80]. These principles are based on the *Fair Information Practice Principles* (FIPPs[2]), and were updated in 2013 in a document titled *The OECD Privacy Framework* [OEC13]. The revised OECD guidelines include additional obligations on data controller operations, audit processes, and more emphasis on the controller's accountability. The following eight basic principles are extracted from the OECD 2013 guidelines [OEC13], which are known as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*:

1. **Collection Limitation:** there should be limits to the collection of personal data and any data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality:** personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose Specification:** the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation:** personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Purpose Specification item, except: a) with the consent of the data subject; or b) by the authority of law.

[2] http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

5. **Security Safeguards:** personal data should be protected by reasonable security safeguards against risks of loss or unauthorised access, destruction, use, modification or disclosure of data.

6. **Openness:** there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation:** individuals should have the right to:

   (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

   (b) have communicated to them, the data relating to them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to them;

   (c) be given reasons if a request made under items (a) and (b) are denied, and to be able to inquire such denial; and

   (d) inquire data relating to them and, if the inquire is successful, have the data erased, rectified, completed or amended.

8. **Accountability:** a data controller should be accountable for complying with measures which give effect to these principles.

1.3.2 Canadian Standards Association Model Code - CSAC

Canada has a well-accepted model code of conduct with respect to privacy, called the *Canadian Standards Association Model Code - CSAC for the Protection of Personal Information* [CSA96]. It was developed based on the existing OECD Privacy Guidelines [OEC80] by the Canadian Standards Association, which is Canada's major organization for standards development and certification. The CSAC is the basis of the Canada's federal law on the topic of data privacy, called Personal Information Protection and Electronic Documents Act (PIPEDA).

The CSAC was adopted by the Government of Canada in 1996 and reaffirmed in 2001. Nowadays, it is representative of the principles behind privacy legislation in many nations and is used as the privacy standard basis for practical application in various specific contexts of data protection [YK05]. The following describes the ten privacy principles of the CSAC [CSA96]:

1. **Accountability**: an organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance in relation to the privacy principles.

2. **Identifying Purposes**: the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**: the knowledge and consent of the individual are required for the collection, use or disclosure of personal information.

4. **Limiting Collection**: the collection of personal information shall be limited to the purposes identified by the organization. Information shall be collected in a fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**: personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy**: personal information shall be as accurate, complete, and up-to-date as is necessary for the intended purposes.

7. **Safeguards**: security safeguards appropriated to the information sensitivity shall be used to protect personal information.

8. **Openness**: an organization shall make readily available to individuals specific information about its policies and practices related to the management of personal information.

9. **Individual Access**: upon request, an individual shall be informed of the existence, use and disclosure of her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance:** An individual shall be able to inquire the organization's compliance with respect to any aspect of the CSAC Code, and the organization must respond to all inquiries and complaints.

1.3.3 European Data Protection Directive 95/46/EC

In Europe, personal data protection is currently described by a set of regulations centred around the Data Protection Directive 95/46/EC (i.e., *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*) [PtC95]. This Directive specifies extensive data protection goals to be reached by institutions, organization and people within E.U., imposing broad obligations on those who collect and control personal data. Each E.U. member must implement the Directive, but has a certain degree of freedom on how it is implemented. Examples of implementations of the Directive are the Italian's *Codice in materia di protezione dei dati personali* [Leg03], the French's *Loi relative à l'informatique, aux fichiers et aux libertés* [fra78], and the United Kingdom's *Data protection act* [otDPC98]. The current Directive only applies to organizations that either process personal information of European citizens or makes use of information systems within the E.U. The following describes the nine principles of the Directive 95/46/EC [JL00, Nar03]:

1. **Intention and Notification:** the processing of personal data must be reported in advance to the Data Protection Authority or a personal data protection official, unless processing has been exempted from notification.

2. **Transparency:** the person involved must be able to see who is processing her personal data and for what purpose.

3. **Finality**[3]: personal data may only be collected for specific, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.

4. **Legitimate Ground for Processing:** the processing of personal data must be based on a foundation referred to in national legislation, such as permission, agreement, legal obligation, justified interest and such like. For special data, such as sensitive data, stricter limits prevail.

5. **Quality**[4]: the personal data must be as correct and as accurate as possible, sufficient, to the point and not excessive.

6. **Data Subject's Rights:** the data subjects involved have the right to peruse and to correct their data as well as the right to raise objections.

7. **Security:** providing appropriate security for personal data held within information systems is one of the cornerstones of the Data Protection Directive. Measures of technical and organisational nature suitable and proportional to the sensitivity of the data, as well as possible risks with potential harms, should be considered to avoid misuse or disclosure of personal data.

8. **Processing by a Processor:** if processing is outsourced to a processor, it must be ensured that the processor will observe the instructions of the controller.

9. **Transfer of Personal Data Outside the E.U.:** in principle, the traffic of personal data to a country outside the E.U. is permitted only if that country offers adequate protection.

In 2012, the European Commission proposed a reform of the E.U.'s data protection rules to cope with new technologies in social networks and cloud computing [CP12]. The new rules are expected to be officially released in 2015 or 2016 under the name "General Data Protection Regulation" (GDPR) [PtC13c], and is intended to replace the current Data Protection Directive [PtC95]. The new aspects of the proposed GDPR include:

- *Informed Consent (Art. 4)*, which grants individuals the right to be always informed and fully aware about what data is being processed;

[3] *Finality Principle* corresponds the so-called *Purpose Principle*, which states that data may only be collected for specified, explicit and legitimate purposes.

[4] *Quality Principle* corresponds the so-called *Proportionality Principle*, which aims to guarantee that the collected personal data is adequate, relevant and not excessive in relation to the purposes for which they are collected or processed.

- *Transparency for data handling and communication (Art. 11)*, which grants individuals the right to be informed on what is done with their information;
- *The right to erasure (Art. 17)*, which grants individuals the right to request the erasure of personal data, thus avoiding further data processing;
- *Regulation of profiling (Art. 20)*, which grants individuals the right to not be characterized based on profiling;
- *Data protection by design and by default (Art. 23(3) and (4))*, inspired by the "privacy by design" approach. The aspects of privacy by design mostly stressed in the GDPR are privacy by default and privacy all along the lifecycle of the system; and
- *Data protection impact assessments (Art. 33)*, which have to be conducted when processing operations present specific risks to the rights and freedoms of data subjects. The risk-based approach should be an important criterion to determine obligations and safeguards for a controller and a processor.

1.3.4 Comparative Analysis

The data protection frameworks OECD (section 1.3.1), CSAC (section 1.3.2) and Directive 95/46/EC (section 1.3.3) have similar principles, even though they may differ in the terminology and on how the overlapping concepts are divided. They address the way in which organisations should collect, use, and disclose personal information, the right of individuals to access information about themselves, and if necessary to correct this information.

In the scope of these regulatory data protection frameworks the users' consent legitimates the use and process of personal data, as suggested by principles OECD.1, CSAC.3, D.4. The latest definition of consent is provided by the GDPR in article 25: *"Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data"* [PtC13c].

Also, these frameworks introduce distinct responsibilities between data processors and data controllers. The concepts of "controller[5]" and "processor[6]" appear as distinct features within OECD, Directive 95/46/EC and GDPR. Often, these concepts are difficult to apply in practice because of the complex relationships between them when processing personal data [Als12]. Conversely, the CSAC do not make a distinction, regarding responsibilities, between data processor and data controllers. In the Directive 95/46/EC and the GDPR, controllers and processors are involved in the transfer of personal data to other countries outside the E.U., and both must provide an adequate level of protection according to the principle *Transfer of Personal Data Outside the E.U.* Thus, the territorial space of these data protection systems

[5]Controller decides the purposes and use of the processing of personal data.
[6]Processor processes personal data on behalf of the controller.

extends beyond the European territory. An alignment of the principles of OECD, CSAC and the E.U. Directive 95/46/EC is proposed in the Table 1.1.

In order to assist the development of CSAC compliant code, a handbook called "Making the CSA privacy code work for you" was proposed. Similarly, aiming to clarify and guide the application of the Directive 95/46/EC for all member states of the E.U., representatives of Data Protection Authorities composing the European Article 29 Working Party have been providing many documents with opinions and advices on data protection and privacy since 1996.

1.4 Digital Privacy Attacks

Protecting individuals' privacy when sharing data is a challenging task. In the 90s, personal and sensitive information was protected using anonymization techniques when storing and disclosing data. However, various privacy attacks allow the re-identification of individuals. Famous examples are the identification of the medical records of the governor of Massachussetts [Swe97], the identification of the history of Thelma Arnold in the AOL query records [BJ06], and the re-identification of individuals in the Netflix prize training data set [NS08]. Lately, new computational techniques (from big data to ubiquitous Internet) have increased the vulnerability of individuals to online attacks, since huge amounts of personal data can now be easily organized, processed and disseminated. By combining just a few pieces of data, it is possible to identify people or trace their behavior [EC15].

This section explores three kinds of digital attacks (tracking, profiling and identity theft) that are well-recognized in the context of the Internet services such as search engines, social networks, and e-commerce web sites [Cla14, AS11]. Each one of these three current digital attacks are results of the combination of privacy violations that were not explicitly addressed in Solove's taxonomy.

1.4.1 Tracking

Tracking is the activity of following people's activities and interactions. One of the major threats about privacy on the Web is the users' traceability, generally used by organizations for advertising purposes [MS11, MSS13, WZ11].

The traditional way of digital tracking is by installing "cookies" that records the websites a user has visited. The tracking is made by storing a unique identifier in the user's browser. Later, when the same user, using the same browser, comes back to the website, the cookies are automatically sent and hence the web server recognises the user (even if she does not log in this website) [Bie13].

In order to comply with contemporary legal frameworks, websites need to advise the user about the presence of cookies and the user needs to give permission before the website stores cookies on her machine. Currently, the majority of web browsers allow users to disable cookies permanently or delete them. However, a Stanford University study[7] stated that half of the 64 analyzed online advertising companies (including Google and Microsoft) do not respect the "do not track" option, even though it is activated. In addition, new tools such as

[7] https://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results

Table 1.1 – Similarities among principles

OECD	**CSAC**	**Directive 95/46/EC**
OECD.1 Collection Limitation	CSAC.4 Limiting Collection CSAC.3 Consent	D.5 Quality D.4 Legitimate Ground for Processing
OECD.2 Data Quality	CSAC.6 Accuracy	D.5 Quality
OECD.3 Purpose Specification	CSAC.2 Identifying Purpose	D.3 Finality
OECD.4 Use Limitation	CSAC.5 Limiting Use, Disclosure, and Retention	D.5 Quality D.3 Finality
OECD.5 Security Safeguards	CSAC.7 Safeguards	D.7 Security
OECD.6 Openness	CSAC.8 Openness	D.2 Transparency
OECD.7 Individual Participation	CSAC.9 Individual Access	D.6 Data Subject's Rights
OECD.8 Accountability	CSAC.1 Accountability CSAC.10 Challenging Compliance	D.8 Processing by a Processor D.1 Intention and Notification D.9 Transfer Outside the E.U.

super-cookies[8] and web bugs[9] can track the mobility of users' activities in real time, enabling organizations to secretly monitor individuals across multiple websites. Moreover, blocking cookies prevents tracking only by browser-initiated HTTP request, but does not protect from tracking by using scripts or browser fingerprinting [BBJ13].

In the Solove's taxonomy described in section 1.1, Surveillance is in conjunction with Identification activities that can lead to tracking attacks through continuous web monitoring (implicit or explicit) the digital information, which can directly identify person's activities, interactions, and contents.

1.4.2 Profiling

According to an advice paper of the Article 29 Working Party [PtC13a], profiling means *any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behavior, location or movements.*

Profiling is based on the collection and the use of pieces of data to discover correlations between data in databases that can be used to identify and represent a person, and is considered by the Article 29 Working Party as a risky processing operation. The effectiveness of profiling of groups and individuals is usually performed using data mining techniques [Sch11]

Poo et al. [PCG03] categorise profiling in two types (static and dynamic). *Static profiling* is the process of analyzing user's static profile and predictable characteristics. However, static profiling degrades in quality over time. *Dynamic profiling* is the process of analyzing user's activities or actions to determine her personal interests. Data from these profiles are commonly organized into seven categories: demographic, geographic, technical, predictive, psychographic, behavior and life event [RSS14]. Given the variety of data presented in the profiles, companies can use profiles information on their own behave (e.g., targeted advertising for monetization). In Solove's taxonomy described in section 1.1, Aggregation along with Identification, Secondary Use and Disclosure activities can lead to profiling attacks. Profiles are digital portraits of aggregated fragments of information that directly correspond to a person, revealing unknown facts about her life as well as being used in other contexts, besides the original proposal from which information was collected.

1.4.3 Identity Theft

Identity theft is a crime of stealing a person's personal data (e.g., SSN, credit card number, online banking login, password, amongst others) and acquiring benefits using the victim's identity [Sol03, Kar12]. Karuppanan [Kar12] identifies five categories of identity theft: business (using another's business name to obtain credit cards or checking accounts), criminal (posing as another person when apprehended for a crime), financial (using another's identity to obtain credit, goods, and services), medical (using another's identity to obtain medical

[8] Super-cookies are a type of browser cookie that is designed to be permanently stored on user's computer.

[9] Web bug is an HTML element in a web page or email that is intended to be unnoticed by users, but allows to check that a user has visited a page or email.

care or drugs) and identity cloning (using another's information to assume her identity in daily life). A possible consequence for this criminal activity is to harm a real person's reputation by destroying her credibility. A thief may obtain personal information from database companies, public records and social network websites. It is one of the most rapidly growing and troubling information privacy problem and has been at the top of the list of consumer complaints of the Federal Trade Commission (FTC) for thirteen consecutive years[10]. Furthermore, based on the Javelin report[11], in 2012 there were more than 12 million victims, a total of 21 billion dollars loss only in the U.S. In Solove's taxonomy described in section 1.1, Insecurity together with Appropriation activities can lead to Identity Theft, which occur when person's identity has being modified or used by others.

An adequate level of data protection requires the implementation of measures towards minimizing or eliminating the undesirable processing of personal data.

1.5 Privacy Enhancing Technologies

In digital information environments, privacy protection can be improved by the means of **P**rivacy **E**nhancing **T**echnologie**s** (PETs). A formal definition of PETs was provided by Holvast [Hol09]: "*a coherent system of information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing the unnecessary undesirable processing of personal data without losing the functionality of the information system*". There are a wide variety of PETs available and some attempts to provide a comprehensive classification [DAM06, Gol07]. However, classifications established at this time could not take into account important developments made in the recent years with regards to PETs, such as the evaluation of the level of privacy protection proposed by modern privacy metrics, which is relevant to privacy in databases. More recently, Fischer-Hübner and Berthold [FHB13] provided a taxonomy for PETs into three categories: PETs for minimization, PETs for the safeguard of lawful processing, and the combination of both. While this taxonomy includes new available technologies, it is difficult to differentiate the various PET functionalities in this taxonomy. Therefore, rather than using any available classification in the literature, this section highlights the development of PETs based on functionalities along with their application scenarios. PETs are organized in six groups: protection of user's identity in email systems, protection of user's identity when accessing interactive systems, protection of user's content, protection for identity management, protection for privacy policy management and privacy protection in databases.

1.5.1 Protection of User's Identity in Email Systems

The first group of PETs is related to protection of the identities of Internet users using email anonymity and pseudonymity systems. Email anonymity systems allow a user to send email without revealing her personal information such as identity, email address, or IP address. Email pseudonymity systems also allow the user to set up a persistent pseudonym, which can

[10] lifehacker.com/five-steps-to-take-immediately-if-youre-the-victim-of-1507265334
[11] https://www.javelinstrategy.com/news/1387/92/1

be used to receive email as well. These PETs, such as described by Goldberg [Gol07], can be classified in four types of remailers. **Type-0 Remailers** are the oldest and simplest systems for email anonymity. This remailer removes the original email address of the sender and assigns a pseudonym, and then forwards the email to the receiver. The most well-known type-0 remailer is anon.penet.fi. **Type-I Remailers** are based on the same principles of Type-0 but with a number of improvements, such as chaining (messages are sent through a "chain" of multiple and independent remailers), encryption (incoming and outgoing messages are encrypted to avoid observers following the messages through the chain) and mixing (incoming messages to a remailer are batched together and randomly reordered before they are sent out). **Type-II Remailers**, also known as Mixmaster Remailers, address problems identified in Type-I remailers by providing enhanced protection against size correlation and replay attacks. In order to defeat size correlation attacks, Type-II remailers divide all messages into packages of various sizes which are sent separately through the network of remailers. Defence against replay attacks works by remembering which messages the remailer sent, and not sending out the same message more than once. **Type-III Remailers**, or Mixminion Remailers, improve Type-II Remailers features and include a better system for handling replies to anonymous messages and protection against replay attacks.

1.5.2 Protection of User's Identity when Accessing Interactive Systems

The second group of PETs is related to *protection of user's identity when accessing interactive systems*. A number of PET technologies have been developed to enhance privacy using web proxies for interactive services, such as instant messaging, reducing as much as possible the correlation between input and output data to keep users anonymous. There are three main softwares that reduce association between users and the related data, implemented using MIX techniques [Gol07]: Anonymizer, Onion Routing and Tor. MIXes are routers that hide the link between incoming and outgoing messages. Pfitzmann et al. [PSS+07] define MIX nets as a chain of proxies following one just after another. **Anonymizer** is a system corresponding to one single MIX to provide anonymity protection for Web browsing by hiding information from end servers. It is one of only a few commercially successful anonymity technology, providing a simple, low-cost system along the lines of the Type-0 remailers. **Onion Routing**, which is based on the concept of MIX-networks, was originally developed by the U.S. Naval Research Lab. Its use was primarily for anonymizing web traffic, and also to allow users to anonymously connect to any TCP/IP server on the Internet. Similarly to remailers, a path is created through several Onion Routers around the Internet. Unlike remailers, the path is "long-lived": data is anonymously delivered and replies are returned along the path. After the communication is completed, the path is turned down. **Tor** is the most successful interactive anonymity tool: hundreds of thousands of users send about 8 terabytes of data per day through hundreds of Tor nodes. The Tor network consists of several servers called Tor nodes. Each node only knows its predecessor and its successor. It is the most famous implementation of the Onion Routing project. In addition to protecting users, Tor also protects the privacy of providers of TCP/IP-based services: a user may run a web server anywhere in the world, which can only be accessed through Tor, and Tor protects the identities of the user and the provider of the service. However, one of the most notable drawbacks is that Tor reduces the

speed of web browsers.

1.5.3 Protection of Users' Data

The third group of PETs is related to *protection of user's content*. Some of these PETs attempt to protect the stored content of users' through encryption. One popular program which allows to encrypt data is Pretty Good Privacy (PGP), which is used to protect stored data files. Furthermore, PGP also attempt to protect the content of users' private communication through encryption. In this context, **PGP** is used to encrypt or digitally sign email messages. Users install PGP-compatible software and use it to encrypt email before sending it. Many email programs have incorporated PGP support. PGP has been available in some form for more than 25 years. Another PET that encrypts communication is Transport Layer Security (TLS), which has replaced Secure Sockets Layer (SSL) [Gol07]. **SSL** is a protocol developed by the Netscape company[12] to transmit private documents via Internet using a cryptographic protocol. Every major web browser comes with in-built support for these technologies and their use is largely invisible to the user, where no special installation or configuration is necessary. In addition, other PETs attempt to guarantee private computation over protect data. Secure multiparty computation and homomorphic encryption are two significant examples. **Secure multiparty computation** protocols allow a set of n parties $(p_1, ..., p_n)$, each with their private inputs $(x_1, .., x_n)$, to compute an agreed arbitrary joint function $y = f(x_1, .., x_n)$ [CCD88, GMW87]. The idea behind secure multiparty computation is based on the "millionaire problem" [SMK11]: two millionaires wish to compute which one is richer, but without revealing to each other how much money they have. Secure multiparty computation is today used as a practical solution to various real-life problems, such as distributed voting, private bidding and auctions. **Homomorphic encryption** is a form of encryption that enables to perform mathematical operations on encrypted data (additions or multiplications), without the necessity to decrypt the data. The first homomorphic systems were called *partially homomorphic* because they supported either adding or multiplying encrypted ciphertexts, but not both operations at the same time. Examples of partially homomorphic encryption algorithms are Goldwasser and Micali [GM82], El Gamal [EG85] and Paillier [Pai99]. The problem of a *fully homomorphic* encryption scheme supporting arbitrary functions was recently solved by the breakthrough work of Gentry [Gen09]. Following Gentry's framework, other fully homomorphic schemes have been presented [SV10, vDGHV10]. Such schemes could be useful in theory for cloud computing security: an Internet user sends encrypted data to a server in the cloud, data is then processed without decryption and sent back in a still-encrypted format. However, the fully homomorphic solution is likely to remains impractical in real life scenarios because of the intractable size of the keys and ciphertexts involved.

1.5.4 Anonymous Credentials

The fourth group of PETs is related to anonymous credentials. These PETs are also available to provide authentication (or authorisation) without user's identification. In many on-line

[12] http://isp.netscape.com

systems operations involving payments (e.g., baking online payment), secure payments transactions that require protection of user's identities is a important demand. Deswarte and Melchor [DAM06] highlight two examples of credential systems: Electronic Cash and IDEMIX. **Electronic Cash**, or e-cash, is a particular kind of anonymous credential system, in the sense that it enables performing financial operations without being disclosed. In this application, a cryptographic technique called "blind signature" was introduced by David Chaum's together with the concept of untraceable electronic money, which allow users to hide the contents of a message before it is signed and to recover the original document with a valid signature afterwards [DAM06]. The IBM **IDEMIX** (Identity MIXer) is a system for strong anonymous or pseudonymous credentials. IDEMIX is a library of cryptographic protocols and data formats that are the result of the IBM research work on various useful security protocols. IDEMIX has been used in large research projects, such as the PRIME[13] project, and has the purpose of attestation of personal properties using "zero-knowledge proof". **A zero-knowledge proof** is a cryptographic protocol by which a *prover* assures to a *verifier* the validity of a statement, without having to reveal any other information about the statement being proven [GMR85, GMR89], thus keeping the secret of the statement and accomplishing the attestation of the desired property. Zero-knowledge proofs fulfil the following three properties [FHB13]: completeness (if the statement is true, then the honest verifier will be convinced of this fact by an honest prover), soundness (if the statement is false, then no cheating prover can convince the honest verifier that it is true, except with very small probability), and zero-knowledge (if the statement is true, then no cheating verifier learns anything other than this fact). Zero-knowledge proofs can be used to allow anonymous attestation or authorization in devices, such as RFID tags and passports.

1.5.5 Privacy Policy Management

The fifth group of PETs is related to *protection for privacy policy management*, which includes languages to specify, to exchange, to negotiate and to enforce access control privacy polices. Examples include the Platform for Privacy Preferences (P3P), the eXtensible Access Control Markup Language (XACML) and the Enterprise Privacy Authorization Language (EPAL). **P3P** is a declarative language that expresses websites' privacy policies in a machine-readable format, enabling web browers to read P3P policies and communicate them to the user. The main drawback of P3P is the lack of automated enforcement in websites [Con06]. **XACML** is a policy language mainly used for expressing access control. Designed by the OASIS Organization, it defines both an architecture for the evaluation of policies and the communication protocol for message exchanges. However, XACML lacks expressiveness because the "purpose" element is optional, for both data collection and data access [Org14]. **EPAL** is a language to formalize enterprise-internal privacy policies, proposed by the IBM corporation. In EPAL, access decisions are based on a "purpose" element, which plays a major role in personal data protection [IW03].

[13] https://www.prime-project.eu/

1.5.6 Privacy in Databases

The sixth group of PETs is related to *database privacy*. PETs in this category aim to preserve privacy of individuals in database repositories, ensuring that stored data is accessible in a privacy-compliant way. These PETs rely on privacy metrics used to quantify privacy disclosure, and have two aspects [WJ07]: *uncertainty* of the values of individual's personal information (i.e., published data lacks certainty of what private value an individual has); and *indistinguishability* of one individual from the rest (i.e., from the published data the value of some piece of information of an individual cannot be distinguished as higher (or lower) than the value for the rest).

Two of the most relevant privacy metrics include the k-anonymity [Swe02] and the l-diversity [MKGV07]. **K-anonymity** (a kind of indistinguishability) protection of data is met when information for each person contained in the data cannot be distinguished from at least $k-1$ other individuals in the data. However, k-anonymity has two main vulnerabilities: homogeneity and background knowledge attacks [MKGV07]. While the first attack explores the little diversity in the sensitive attribute values and thus the easiness to discover sensitive data, the latter occurs due to previous background knowledge that allows inference on attributes and identity of a person [ZG11]. To overcome these limitations, **l-diversity** (a type of uncertainty) proposes l well-represented sensitive values for each group of records. In l-diversity, sensitive attributes regarding individual's privacy must be diverse within each quasi-identifier group (i.e., set of data records combined with other data to infer individual's identity). **Differential Privacy** is a powerful property on a querying process that provides strong privacy guarantees, independently of the background knowledge of the adversary. Differential privacy ensures that the presence or absence of a single database record does not substantially affect the outcome of a database query. The main idea behind differential privacy is to use noise when answering to an aggregation query, providing protection from the possibility of sampling at individuals and infer precise information about individual entries [Dwo06]. Finally, systems can be developed in which individuals can be identified, but the details of their activities remain secret. For instance, **Private Information Retrieval** is a cryptographic primitive that allows a client to privately recover a record from a (public) database without revealing to the database administrator which specific record is being retrieved [CKGS98]. Thus, private information retrieval provides users with confidentiality regarding her choice of the requested element, and can be very useful when an individual needs to enquire about sensitive topics without being monitored by the database administrator.

The PETs described above can be linked to Solove's taxonomy as countermeasures to prevent privacy violations. It is worth noting that some PETs are able to prevent more than one privacy violation in Solove's taxonomy. For instance, anonymization techniques such as Remailers, Anonymizer, Onion Routing, Tor, E-cash, IDEMIX, Zero-knowledge proofs can prevent Surveillance and Identification activities. Other PETs, such as PGP, TLS, Homomorphic Encryption and Secure Multiparty Computation can be used as countermeasures to Surveillance and Insecurity activities. Privacy preserving database metrics (k-anonymity, l-diversity, differential privacy) can solve privacy violation issues caused by Breach of Confi-

dentiality, Aggregation, Disclosure, Increased Accessibility, and Insecurity activities. Private information retrieval provides guarantees against Surveillance, Disclosure and Exposure. Privacy policies, such as P3P, XACML and EPAL, enable users and other entities to specify how information can be processed and disseminated. Their proper enforcement may then prevent privacy violations in several aspects. Their "purpose" element can also be used to enforce restrictions when information is processed (i.e., avoiding Secondary Use, Exclusion), and disseminated (i.e., avoiding Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Distortion). A mapping of the mentioned PETs onto Solove's taxonomy is presented in the Table 1.2.

In short, PETs have been developed for a number of Internet features, aiming to protect the privacy of individual's and to help organisations to meet their legal and regulatory responsibilities. In fact, PETs can be embedded at the design level to ensure privacy-friendly systems by applying the concept of Privacy by Design.

1.6 Privacy by Design

Legislations and regulatory compliance alone or even the application of PETs are not sufficient to guarantee the enforcement of privacy. In this context, the idea of "Privacy by Design" (PbD) has been growing in relevance in information systems, bridging the gap between the way privacy regulations are expressed in legislation and the development of technical solutions to enhance privacy protection. Accordingly, the utility of PbD has been recognized by the GDPR [PtC13c] and the OECD supplementary explanatory memorandum [OEC13] as a significant subject for the promotion of a deeper understanding of technology, policy and law. PbD inspired the introduction of the Data Protection by Design Principle within the GDPR [CP12], ensuring PbD at every stage of a system design [HT13]. The seven foundation principles of PbD are [Cav10]:

1. **Proactive, Not Reactive; Preventive, Not Remedial:** this principle is characterized by the prevention of privacy-invasive events before they happen, and dictates that privacy protection will be considered and ensured since the beginning of the system.

2. **Privacy by Default:** it seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given information system or business practice. No action is required from the individual to protect her privacy.

3. **Privacy Embedded into Design:** privacy must be embedded into the design and the architecture of information systems and business practices, becoming an essential component of the core functionality.

4. **Full Functionality - Positive-Sum, not Zero Sum:** the system paradigm changes from zero-sum to positive-sum model. In the zero-sum concept, one requirement wins while others lose, leading to inevitable tradeoffs between functionalities (e.g., privacy versus performance). Conversely, a positive-sum describes a situation in which all requirements are implemented together.

Table 1.2 – Solove's taxonomy and PETs mapping

Solove's Taxonomy	**PETs**
Information Collection	
Surveillance	Remailers, Anonymizer, Onion Routing, Tor, PGP, TLS
	E-cash, IDEMIX, Zero-knowledge Proofs, Private Information Retrieval
Interrogation	
Information Processing	
Aggregation	k-anonymity, l-diversity, Differential Privacy
Identification	Remailers, Anonymizer, Onion Routing, Tor, IDEMIX, E-Cash
	Zero-knowledge Proofs
Insecurity	PGP, TLS, Homomorphic Encryption, Secure Multiparty Computation
	k-anonymity, l-diversity, Differential Privacy
Secondary Use	k-anonymity, l-diversity, Differential Privacy, P3P, XACML, EPAL
Exclusion	P3P, XACML, EPAL
Information Dissemination	
Breach of Confidentiality	k-anonymity, l-diversity, Differential Privacy, P3P, XACML, EPAL
Disclosure	k-anonymity, l-diversity, Differential Privacy, Private Information Retrieval
	P3P, XACML, EPAL
Exposure	Private Information Retrieval, P3P, XACML, EPAL
Increased Accessibility	k-anonymity, l-diversity, Differential Privacy, P3P, XACML, EPAL
Blackmail	
Appropriation	
Distortion	P3P, XACML, EPAL
Invasion	
Intrusion	
Decisional Interference	

5. **End-to-End Security, Life-cycle Protection:** security should be embedded into the system prior to the first element of information being collected, and extended throughout the entire life-cycle of the data. This implies, for example, that at the end of the process, all data are securely destroyed.

6. **Visibility and Transparency:** it seeks to assure all stakeholders that whatever the business practice or the technology involved, it operates according to the stated promises and objectives, being also subject to independent verification. Its component parts and operations remain visible and transparent to the users and the providers.

7. **Respect for User Privacy:** it requires that architects and operators keep the interests of the individual uppermost by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

PbD is a process in which these principles provide the basic properties that a system should have to build privacy directly into the design. Principles 1-3 provide useful guidance about the recognition that privacy issues must be given early in the design process, which is a cost-saving measure in the development of information systems. The leading principle of Privacy by Default is a powerful measure towards data minimization within proactive organizations, which states that collecting personal data should be minimized. Principle 4 may seem unrealistic due to the fact that privacy is not an unlimited and absolute right, as it can be in conflict with other rights and requirements. Principle 5 emphasizes secure techniques and organizational policies of safeguard of user's shared information against leakage, which is a key aspect of many PETs' engineering. Principle 6 reinforces freedom of information and transparency, promoting openness with regards to processing operations. The last principle states that privacy should be user-centric, giving to the user flexible options to control personal data and notice about how information is handled.

In this thesis, the PbD approach is embraced as a way to ensure satisfactory levels of privacy protection. Indeed, systems designed over these principles tend to be more effective for safeguarding personal information.

1.7 Conclusion

In democratic societies, privacy is an important right to be respected and protected with proper measures. Privacy protection between organizations and Internet users provides control over data, establishes how data shall be handled and how potential privacy threats shall be mitigated.

In a fully connected society, privacy protection is provided by technical measures such as PETs, as well as legal regulations. The challenge faced by our society consists in dealing with different aspects of handling personal data in an efficient balance of interests. Organizations must comply with privacy principles, like the OECD, the E.U. Data Protection Directive and the Canadian CSAC policies, which should describe the privacy protection practices. The PbD principles play a key role towards the adoption of measures necessary to enforce privacy protection practices within the system design and development, with the intent to

support the integration of PETs, specially on the emerging information systems that pose considerable new challenges with respect to privacy, such as social network applications.

Currently, in massive online communication environments, the aforementioned areas of privacy such as legal regulations, PbD, and PETs are necessary in order to face new challenge in privacy protection, which is mainly related to the impact in Social Network Systems (SNSs), in which users' privacy is always an issue.

Chapter 2

Social Network Systems

Social **N**etwork **S**yste**m**s (SNSs) are online platforms that allow individuals to reproduce on the internet interactions and relationships found in society. Furthermore, SNSs have opened new horizons on the people's communication and on the spread of information. Today it is considered an interdisciplinary topic of research between many different areas, such as computer science, socio-economics and psychology, amongst others.

There are several terms related to SNSs, which can be considered quasi-synonymous. It is worth noting that the different definitions may bring slight nuances and help understand the role of SNSs. For instance, while *social networking* evokes the practice of actively seeking connections (which also happens offline), *online social networks* emphasize online connections, and *social networking websites* focus on connecting to new people. The term *social network websites*, coined by Ellison and Boyd, denotes websites that enable individuals to articulate public lists of connections (i.e., to present a social network and to view others' networks) [EB13].

Social network websites was first defined in 2007 by Boyd and Ellison [BE07] and is probably the most well-known definition for SNSs. Although the 2007's version does not correspond to the current features of SNSs, the same authors provided a more accurate definition in 2013 [EB13]: *"a networked communication platform in which participants*

1. *have uniquely identifiable profiles that consists of user-supplied content, content provided by other users, and system-level data;*

2. *can publicly articulate connections that can be viewed and traversed by others; and*

3. *can consume, produce, and interact with streams of user-generated content provided by their connections on the website".*

In the scope of this thesis, SNSs are defined in consonance with Ellison and Boyd's formal and accurate definition of social network websites [EB13]. However, the term SNSs is used

to represent not only websites but other, decentralized architectures, such as peer-to-peer (P2P) systems, in which all traffic takes place through the P2P network. To explore the potential of SNSs, it is essential to understand the evolution and development of these social organizations.

This chapter introduces the concept, starting with a brief history of SNSs in section 2.1. Then, section 2.2 describes the basic elements, usage and main functionalities of SNSs. Section 2.3 describes current SNSs based on centralized architecture. Section 2.4 describes new architectures that work towards decentralizing infrastructure support. Finally, some conclusion are presented in section 2.5.

2.1 History and Evolution of SNSs

In recent years, SNSs have been constantly growing along with the development of new technologies. The history and the evolution of SNSs can be classified in three periods: the beginning of SNSs (1997–2002), the growth and rise of their popularity (2003–2009) and their consolidation as a global phenomenon (2010–present) [HKP12].

The first well-known SNS launched was SixDegrees[1] in 1997, allowing people to create basic static profiles and relationship lists with friends, as well as sending online messages to others. Attracting around 1 million of registered users in only 1 year, the success of SixDegrees occurred due to the integration of separated services in a single one, such as the use of instant messaging in a social manner among web users. However, the limited business functionalities and the decrease of its use resulted in the fall of the service in 2000 [BE07]. Although unsuccessful, the main basic ideas of SixDegrees marked the beginning of the SNS concept and, since then, many SNSs have been continuously created in a variety of forms, promoting different types of virtual interactions and activities.

Major popularity in SNSs started in the early 2000's. Friendster, founded in 2002, was quickly adopted by 3 million users within the first few months[2]. It was considered the first modern SNS, built on the assumption that friends of friends are more likely to be interested in dating than strangers would be [Boy04]. In 2003, Friendster announced fees to use the website, leading many user to leave it and join alternative, free-of-charge services. Due to technical problems (i.e., the website was not able to handle the rapid growth) and social problems (i.e., users felt embarrassing to find themselves contacting their bosses and classmates alongside their close friends), Friendster rapidly declined in popularity in the U.S. [BE07], even though it has remained popular in Southeast Asia until these days.

During the second period, a new wave of SNSs arose, explicitly seeking narrower audiences, focusing on demographics niches or special interests [HKP12]. The year 2003 corresponds to the incredible growth and success of SNSs, when many companies became famous (e.g., MySpace, Hi5, Xing, amongst others). For instance, professional SNSs such as LinkedIn were founded at this period with a focus on business. Also, the revolution of the Web 2.0 was one of the major impact factors for the popularity and acceptance of SNSs. From 2005 to 2008,

[1] It names derives from the six degrees of separation concept, the so-called "small world". This concept suggested that any two persons are distanced by at most six friendship links [Mil67].

[2] http://www.nytimes.com/2006/10/15/business/yourmoney/15friend.html?pagewanted=all

MySpace was the most visited SNS in the world, due to its widespread adoption by teenagers (a kind of user that earlier SNSs failed to attract). In February 2004, Facebook was launched at Harvard University by Mark Zuckerberg to connect college students, and within the first month more than 19,500 students signed up. Then, Facebook was expanded to other U.S. colleges such as Stanford, Columbia, Yale, New York University and, in September 2006, it was opened to everyone with a valid email address. Also in 2006, Twitter was created as an online microblogging platform enabling users to send posts (tweets). Rather than having "friends", like on MySpace and on Facebook, Twitter users can "follow" other users and also have "followers". As an example of the SNS's connectivity, on January 22, 2010, NASA's astronaut T.J. Creamer sent the first tweet from the outer space, showing how social and geographical boundaries were being reduced. In 2008, Facebook overtook MySpace and became the leader in number of users. Nowadays, the more SNSs are important for business, the more investors are interested in their trade (e.g., MySpace was acquired for US$ 580 million by the media company News Corporation) [BBC05].

The third period is dominated by the maturity of SNSs. Since the early-generation, two decades ago, they are still growing and are part of our daily lives. SNSs are the most visited kind of website worldwide and gather a huge amount of information. Currently, Facebook is the largest and most successful SNS in the world [Hol12], with an actual value of US$ 184 billion[3]. Besides the success of Facebook, there were many SNSs to be launched in the following years. For instance, Unthink started as a rival and anti-Facebook SNS in 2011, focusing on an easier control on privacy. Along with the "anti-Facebook movement", other new approaches that challenged Facebook's hegemony have been focusing on the improvement of privacy through decentralized infrastructures [DBV+10, SVCC09], bringing a new paradigm shift. For instance, Diaspora, launched in 2010 and still in its developmental stages, is an independent open source SNS which works with federated servers. It is the most popular decentralized open source SNS in the world in 2014, with more than 1 million accounts [Dia14]. Figure 2.1 summarizes and presents a timeline of the main SNSs in our history.

2.2 Overview of SNSs

Despite a variety of activities and usage of SNSs, their concepts and structural characteristics are quite similar. SNSs are organized as social structures, made up of a set of users organized as a graph. Each user usually has a profile with her identity, personal information, as well as resources. The social graph represents the social relationships among users in the SNS, the semantics of which may differ from one SNS to another. All these features are the baselines for most SNSs elements and architecture types.

2.2.1 Basic Elements of SNSs

Most SNSs are similar regarding their basic structures and elements, despite of being used for many different purposes. Usually, the main elements are: users, profiles, social graph, resources and services.

[3]http://www.usatoday.com/story/tech/columnist/shinal/2014/03/13/facebook-cracks-market-valuation-oracle-google-apple-microsoft/6343009/

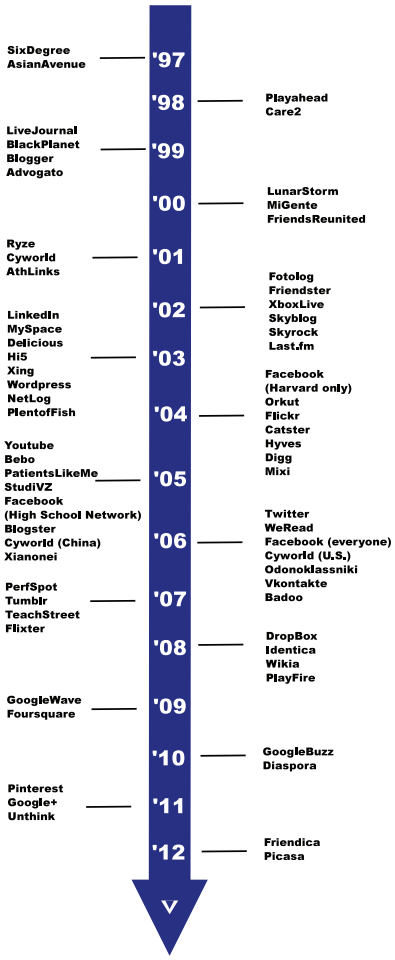

Figure 2.1 – Timeline of the main SNSs since 1997 (adapted from Boyd and Ellison [BE07])

Users are the basic entity in the SNSs, representing individuals and collective social units. Users may provide information about themselves, which constitutes the user's profile.

A user's *Profile* represents the user's identity. The profile attributes include personal information, such as: name, age, gender, and birth day. The profile creation occurs just after the subscription by the user in some SNS, which makes her immediately linkable and visible to the others. Tapiador and Carrera [TC12] surveyed 16 different SNSs (Facebook, LiveJournal, MySpace, Orkut, Twitter, XING, LinkedIn, Flickr, Badoo, deviantART, StumbleUpon, Yelp, Taringa!, Tagged, SoundCloud, Viadeo), and showed that popular profile items are

- Avatar: a picture that represents the user.
- Contact list (also called as friend list): encompasses all contacts of the user.
- Timeline: a summary of recent actions related to the user.

- Wall: allows the user and others to post activities, add or create any type of content within the SNS.

The *Social Graph* is established from social relationships of users within SNSs. Social graph relations can be symmetric or asymmetric [TC12]. To create symmetric (also called bidirectional) relationships, a user sends a "friend request" to another member and, once accepted, establishes a connection where one is allowed to publish in the friend's walls, and vice-versa. To create asymmetric (also called unidirectional) relationships, users do not need "friend requests" to be confirmed, and a user just "follows" (e.g., Twitter) another user. Usually, a social graph may have hundreds of direct and indirect connections to friends, family, acquaintances, and colleagues. Currently, prominent SNSs also provide several ways to help users to build their own social graph (i.e., suggestion of friends or harvesting from address books and other contact lists).

Resources are contents that represent the users' assets. An Asset for a user is a collection of relevant pieces of content, shared with or by the user. Users can upload, add or create contents onto their webspace that are generally personal and sometimes sensitive data. Examples of these contents are: profiles, social graph, messages, pictures, videos, amongst others.

Most of the current SNSs have a myriad of internal *Services*, such as news, games, applications, and tagging. To enable communication between users, SNSs usually offer common messaging services, such as email, chats, text messages, blogging and Internet phone services. Another type of relevant service consists in sharing content (e.g., using "like", "share", "follow" or "send" buttons), which can reveal opinions on a particular subject. Many third-party applications that interact with SNS platforms but rely on external servers offer rich additional services. Two important examples are the Facebook Application Programming Interface (API), which allows members to access many non-Facebook applications [Fac07], and Google's Open Social, which grants applications access to the social graph, as well as messaging service and feeds [Goo07]. The greatest advantage of Google's Open Social over Facebook API is the interoperability with other SNSs.

These common basic elements allow users to present themselves and interact in a efficient manner within the SNS. Hence, users can get the benefits associated to different types of SNSs such as work, family, amongst others.

2.2.2 Usage Profile Categorization

A wide variety of people can be served by many categories of SNSs. For instance, these categories can be organized as "personal, professional, interest, and functional" [Ho12], or as "private, business, general and special interest" [HKP12]. Another option, stated by Lovetoknow[4], summarizes these categories as "informational, professional, educational, hobbies, academic and news".

Although none of the above classifications provides complete and non-overlapping categorization, Beye et al. [BJE+10] provide a very comprehensive classification that leads to a broad picture of several types of SNS into two categories: Connection and Content.

[4]http://socialnetworking.lovetoknow.com

2.2.2.1 Connection SNSs

The Connection SNSs are user-centric websites with focus on (re-)connecting people and providing social contact. Beye et al. [BJE+10] organize them in four categories: dating, business, enforcing real-life relationships and socializing.

- Dating: helps users to find mates. Each user has a profile to attract potential candidates and connections are typically in the form of love interests, but friendship links are also common and groups can also exist. Traversing is often based on searches or recommendations rather than on existing connections. Messages exchanged between users are often kept private but behavioural information can be kept by the SNS to provide better recommendations. Examples are PlentyofFish and Match.com.

- Business: provides jobs opportunities and business, where user profiles display professional career and education background. In addition, other information can be provided such as past and present professional organizations, awards and distinctions, as well as references. Examples are LinkedIn, Xing and Ryze.

- Enforcing real-life relationships: (re)connection with friends or acquaintances. Examples include family oriented SNSs, colleagues or ex-classmate networks, in websites such as MyLife, Facebook, Friends Reunited and Plaxo.

- Socializing: Fitting the more traditional view of SNSs, with focus on entertainment, where users can connect with friends and find new ones. In order to attract and keep users, this type of SNS usually has a lot of additional functionalities, such as social applications and competitive games. Some examples are Facebook, Orkut, MySpace and Hyves.

2.2.2.2 Content SNSs

The Content SNS are data-centric websites which focus on the content provided or linked by the users. Beye et al. [BJE+10] organize them in six categories: sharing, recommendation, entertainment, advice, hobbies and news.

- Sharing: user-generated content shared within a selected group, such as friends, family, or a far wider number of people. The shared content is usually multimedia (e.g., photo and video) and is uploaded after the user signs up and logs in. Sometimes, access to content also requires login, or knowledge of a hard-to-guess URL. Messages or tags can be added to the shared content. User profiles, if any, are usually brief. Examples are Picasa, Flickr and Youtube.

- Recommendation: SNSs where users do not upload but focus on recommending existing content. Bookreview websites like WeRead.com, and url-tagging communities like Del.icio.us, are examples where the content is discovered, tagged or rated, but not created or uploaded.

- Entertainment: SNSs tied to gaming communities. The profile usually depicts gaming avatars and connections to gaming friends, where messages are sent to other users and sometimes groups are formed. Behavioural information is mostly used to track a user's played games, and unlocked achievements are then displayed in the profile. Entertainment SNSs make money by selling games and game add-ons, or through subscriptions. Examples are Xbox Live, Steam, Facebook and Playfire.

- Advice: SNSs that offer a place for people to share experience or expertise in a certain area, or to seek help and advice. SNSs of this kind exist for medical patients (e.g., PatientsLikeMe), students (e.g., TeachStreet), and software developers (e.g., Advogato).

- Hobbies: SNSs that focus on people who have similar hobbies, interests and preferences, involving recommendations and advices. Examples are AthLinks, Care2, Last.fm and Flixter.

- News: blog-related websites that focus on world news or gossip. Examples of this kind of aggregators are Digg, Twitter, Reddit and Blogster.

It is worth noting that some SNSs are more predominant in some parts of the world than others, which takes into account the cultural background and the user's individual characteristics. A comprehensive list of dominant SNSs (independently of the classification in subsection 2.2.2.1 and 2.2.2.2) according to the continent and the region is provided by Gharibi and Shaabi [GS12] and is presented in the Table 2.1.

Table 2.1 – Dominant SNSs according to the continent and the region

Continent/region	**Dominant SNSs**
Africa	Facebook, Hi5
America (North)	Facebook, MySpace, Youtube, Flicker, Netlog
America (Central & South)	Facebook, Orkut, Hi5
Asia	Friendster, Orkut, Xianonei, Xing, Hi5, Youtube, Mixi
Europe	Facebook, Badoo, Bebo, Hi5, Xing, Skyrock, Playahead, Odnoklassniki, Vkontakte
Middle East	Facebook
Pacific Island	Bebo

2.2.3 Functionalities of SNSs

A general functional model of SNSs can be depicted by multiple layers. Pallis et al. [PZYD11] proposed to describe SNSs' basic functionalities in five layers: hardware infrastructure, operating system, data storage, content management and application. Similarly, Datta et al. [DBV+10] also proposed five layers: physical communication network, distributed or P2P

overlay management, distributed or P2P storage systems, social network support and application. Another option, stated by Cutillo et al. [CMS10], summarizes the layers in: social network, application services and transport. All these functional models have very similar layer components for different functions. In this thesis, SNSs are structured in two main functionalities: architectural services and storage, as presented in Figure 2.2.

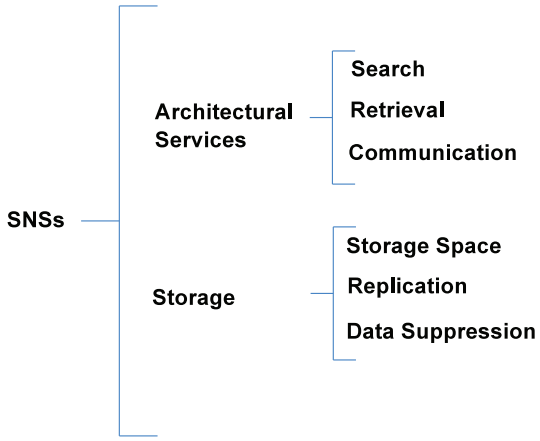

Figure 2.2 – Functionalities of SNSs

- Architectural services: covers the main services provided by the SNS, such as search, retrieval and communication. *Search* is the mechanism to locate data and users in SNSs. *Retrieval* is the mechanism through which data are exchanged among entities (users, service provider and third-parties). *Communication* determines how data are transmitted among entities.

- Storage: describes how information is kept in the system, especially the content that a user uploads to the SNS, such as pictures, personal data, amongst others. *Storage space* specifies where user data are stored, *replication* indicates which entity is in charge of replicating profiles and resources, and *data suppression* specifies which entity has the power to delete data from the system (for instance, when a user closes their account).

These functionalities can be implemented in a centralized or a decentralized fashion, depending on the preferences of the designer.

2.3 Centralized SNSs

Today, most SNSs rely on centralized storage and architectural services. Centralized SNSs are web-services that have a strongly hierarchical architecture, and a single and central authority with exclusive administration control. It is responsible for gathering information, maintaining all user information and relationships. These centralized SNSs are typically implemented as client-server applications, in which the central authority is required to manage the activities

of users, being in charge of communication routing, searching friends and data, and content retrieval on behalf of the users, which includes the utilization of common hardware and software platforms. An important advantage of a centralized SNSs is the facility of updating and maintaining the system. Some of the most common examples are Facebook, Twitter, LinkedIn and MySpace.

The client-server paradigm is the most popular architecture in the Internet. A centralized server is usually a computer with huge memory, processing power, including high speed and storage capacity. Servers accept requests from various clients and perform all processing operation tasks before sending a response. Clients are users' machines, which communicate with a server to request resources or services, and the server responds to those requests [SJB11].

The centralized management repositories are in charge of maintaining and storing all users information and relationships. These data collections are concentrated within a cluster or data center. It contains valuable collection of private information of user profiles (e.g., opinions, details, and other user-generated content), which is very useful for the advertising industry [PBS11]. The business model of centralized SNS is usually based on advertising to make profits and revenues, where the value of the SNS increases as the number of members rises [PZYD11].

The service provider may allow users to specify their privacy preferences, but the enforcement of these users' privacy policies is over his responsibility. In case of client misbehaviour, the provider is the accountable authority to deal with complaints, with the power to remove inappropriate contents or to ban users.

An important example among centralized SNSs is Facebook, founded by Mark Zuckerberg in 2004. Facebook is the most popular online destination with more than 1.32 billion active subscribers, who spend a daily average of 20 minutes on the site. This SNS focuses on the entertainment and socializing scopes. In the registration step, the user chooses a username and password. Then, the user establishes connections that can be based on email addresses, joint groups, existing connections, particular search terms, etc. Facebook tries to make easy how people can find a specific user in the SNS, setting by default the user name, profile picture, gender and networks visible to everyone. The user can also post content (photos, videos, links) to her wall or to another wall, and send messages to other members. Popular applications include sharing images, videos, favourite links, wall-posting and personal information. Facebook provides integration to other SNSs and to mobile applications such as iOS and Android. *Architectural Services* provided by Facebook to users are mainly based on a centralized architecture where search, communication and information retrieval services are operated by a central entity, the service provider at Facebook, and only the result is provided to users on the client side. It is worth noting that even though Facebook services are clustered and distributed for the sake of performance and load balancing, they are all controlled by a single entity. *Storage* is centralized in Facebook's cluster of around 180,000 web and database servers. Facebook replicates the complete user profiles across their data center. Data suppression does not seems to be completely implemented [AGR13], because Facebook apparently remains with users' data for an undetermined time [MAYLL$^+$09], arguing safeguard against legal measures.

2.3.1 Discussion about Centralized SNSs

Centralized SNSs rely on the ease-of-use for least skilled users. They can easily share information, pictures, videos or any subject of interest, meet new people and make new contacts with different cultures around the world. Moreover, SNSs are a central place for business opportunities and entertainment with different applications, offered by the service provider and third-parties: on the one hand, centralized approaches are highly valuable for business based on economic models where revenue flows from the advertiser to the service provider. On the other hand, the provider opens important information about users to the advertisers.

Even though several advantages to users that seems very attractive are presented by centralized SNSs, some limitations highlight serious concerns. According to Baran [Bar64], centralized networks are vulnerable to disruption because the provider's web-server is a single point of failure. Other disadvantages are the lack of integration and portability: each centralized SNS requires the user's subscription by demanding personal information and rarely allows to leave the system with her information. Also, the provider is surveillance on profiles of user are almost inevitable.

From the point of view of the centralized storage and control of information, the main identified shortcomings are:

- Service providers do not allow much control for the users on how their personal data are collected, used and disseminated. Users cannot control inappropriate disclosure of what others may reveal about them, which are not limited to their identity [AGH10, AGH09, MAYLL+09].

- Service providers have unlimited access to the users' information [BSVD09, AGH10]. Specifically, the central authority imposes a global policy, even thought every single user may also have her own. The latter are not on the same level and the central authority may constrain them.

- The service provider can change the terms of service [BL09]. The provider could arbitrarily adapt its privacy policies or the usage of user data, allowing further information sharing with minimal user notification.

- Users have to agree to the policies of the SNSs when using their services [MAYLL+09]. This agreement between the service provider and each user is essentially a "take it or leave it" contract, where generally only one side has all the power and may use it to take an advantage. By accepting the terms and conditions of use, users give consent and legitimize nearly any form of collection and use of personal data.

- Privacy settings provided by SNSs have proven difficult to use [ARG11, BL09, Cra03]. It is not clear to the user how to use the SNS settings. Moreover, their privacy policies are long and complicated to understand. For instance, Facebook privacy policies contains 6,857 words and 11 pages with single spacing. Similarly, LinkedIn privacy policies contains 6,827 words and 14 pages with single spacing. Thus, most of people do not read it because it is a time-consuming task.

- SNSs may explore user profiles for data mining and target advertisement [BSVD09, CMS09, SD12]. In this context, Barbier and Liu [BL11] present the most common data mining applications related to SNS, which are: group detection (finding and identifying a group), group profiling (identifying what is the group topic), and recommendation systems (recommend new friends or new groups to a user). By using data mining techniques, these SNSs allow companies to take advantage of user information for advertising purposes, constituting the most important source of their revenue. For instance, Facebook's Beacon program[5] reports and displays back user information from third-party websites, such as Amazon.

2.4 Decentralized SNSs

To achieve stronger control, many efforts have been made towards the decentralization of SNSs. Decentralized SNSs are social networks implemented on a distributed information management platform. They have been proposed along the last five years in the literature to avoid or skip the centralized service provider. Indeed, by decentralizing SNSs, the concept of a service provider may be replaced by a set of peers. These several entities distribute the control and the storage, sharing the task to run the system, which includes the enforcement of privacy policies [DBV+10].

Decentralizing the existing functionalities of SNS deals with a significant number of challenges since parts of the SNS, or even the whole SNS, are no longer centrally operated. Buchegger and Datta [BD09] discuss nine design challenges towards decentralization: Storage, Updates, Search and Addressing, Topology, Openness to New Application, Security, Robustness, Limited Peers and Locality. In decentralized SNSs, finding ways to maintain data availability when the owner of the data is offline and determining the necessary number of replicas to host a user's profile becomes crucial in order to distribute the *Storage* of data. It is typically achieved through redundancy, assuming that the friends of a user is capable to provide sufficient storage capacity to all the published data. In distributed storage and replication schema, it is difficult to efficiently disseminate social updates among peers, specially if their time zones are different. *Updates* take into account the latency between the end of an update event at a certain replica of a user data and its arrival on another replica. Similarly, *Search and Addressing* is related to updates, in a sense that users should be able to discover their friends from real relationships as well as contents concerning their interests. After the friend is located, it is important to establish how users may be connected, forming the SNS *Topology*.

In addition, an open challenge relies on how decentralized SNSs enable *Openness to New Applications*. While openness to third-party extension potentially provides benefits for the users, it is a risk of exposure to untrusted applications. In decentralized SNSs, if some user chooses to enable a third-party application such as a game, her choice should not affect other users or even users directly connected to her. In order to keep control over data, *Security* measures need to be applied. A particular security measure is to encrypt the user's distributed storage and authorize only some users to access content. In such encryption and

[5] http://www.pcworld.com/article/140182/article.html

access control mechanisms, it is important to manage key distribution and maintenance, as well as a fine granularity of access control, to determine who can read, write, modify or delete each shared piece of data, and how to enforce these decisions. Along with security issues, another challenge is *Robustness* against misbehaviour and failures. In fact, decentralized SNSs lack an accountable authority to deal with complaints and unreliable users is still an important open issue.

In order to take advantage of the decentralized nature of the SNS, a user may want to communicate directly by taking advantage of her *Locality*. Mapping physical location to the virtual network may allow mobile applications to directly exchange data using physical proximity. The incentives to make the user an active participant, running the infrastructure in a decentralized SNS, is the major challenge for the decentralization widespread adoption. The feasibility of the decentralized approach depends on the *Limited Numbers of Peers* to run the core network at the same time, allowing clients to access its services.

These functional aspects are implemented through distinct degrees of decentralization and can be classified in three categories: networks of trusted servers, P2P systems, and hybrid systems. These scopes of decentralization range from partially decentralized, to hybrid, to entirely decentralized systems and have been mainly developed in the research community.

2.4.1 Networks of Trusted Servers

The first attempt at developing SNSs in a decentralized fashion was based on a network of trusted servers. In this context, the servers infrastructure is distributed and the user is able to decide in which server her data will be stored [PBS11]. Some examples of SNSs based on this architecture are

- Friend-Of-A-Friend (FOAF[6]): FOAF is an ontology to describe people by their attributes (`foaf:person`) including name, nickname, email, etc. Social connections are described by a number of sub-properties of (`foaf:knows`) including parentOf, siblingOf, friendOf, etc. In 2009, Yeung et al. [MAYLL+09] proposed a SNS where users can manage their own personal social network profile information by using the FOAF ontology on a trusted server. A FOAF profile is stored in a trusted server. Then, to access user data, application and friends need to be authenticated throughout different servers and may also login in to different SNSs by using the same digital identification. This approach attempted to improve data interoperability, since FOAF profiles can be connected across different SNSs. *Architectural Services* in FOAF are performed by users for retrieval, communication, and search by using the "foaf:knows" property. More specifically, communication is performed using "foaf:knows" and "rdfs:seealso" properties to connect distinct FOAF files together. *Storage*, in the FOAF framework, does not implement replication techniques and a user directly stores her FOAF profile in a trusted centralized server. In the FOAF specifications, data suppression is not mentioned.

- Diaspora[7]: Diaspora is an open-source SNS project based on a decentralized architec-

[6] http://www.foaf-project.org/
[7] http://diasporaproject.org/

ture that uses independent and federated servers. The Diaspora network is made by a set of interconnected servers called "PoDs". Users can create private or public PoDs. Public PoDs are connected with a set of clients, called "seeds", in a client-server fashion. Conversely, private PoDs are users' individual servers, without seeds, to manage only their own data. PoDs are in charge of executing all services, such as profile data storage (i.e., local database), contact search by querying other PoDs, and information retrieval. *Architectural Services* in Diaspora are provided by PoDs (i.e., servers) in a decentralized manner. These services include retrieval of profile details for seeds (i.e., clients), search for friends in other PoDs, and communication within the SNS. *Storage* is decentralized in the PoDs. PoDs provide storage space, and users are able to decide on which PoDs their information will be stored. PoDs replicate a user's data through other PoDs that share this user's connection. Data suppression is implemented as soon as a user deletes her account from a PoD, which is propagated to other PoDs that follow her.

This approach allows users to choose which server is dedicated to the storage of their data within an existing distributed infrastructure. On the one hand, the user needs to find a reliable webspace to store data with good scalability [PBS11]. On the other hand, the user can deploy and set up her own web server, and integrate it in the infrastructure, which requires a dedicated server constantly running.

2.4.2 Peer-to-Peer (P2P) Systems

The second category of decentralized SNSs represents a shift from client-server infrastructures to P2P systems. Although P2P are popularly used for content distribution (i.e., sharing of documents and multimedia files), during the last years it has been increasingly adopted for the development of other decentralized applications.

P2P SNSs are composed of user devices without any service provider. P2P SNSs present specific features related to the private nature of the users' profile, the access to their attributes, and the reduced number of friends that can access their files [DBV+10, PBS11]. It is necessary to deal with dynamic relations in terms of online/offline behavior and of adding/removing friends and corresponding access rights. Generally, in many P2P SNSs, encryption is used to ensure confidentiality of private information. Examples of this category are

- Safebook: Safebook is a SNS that uses two complementary components [CMS09] – a Trusted Identification System (TIS) and a specific neighborhood structure (called as *matryoshka*) over a P2P architecture. In a nutshell, a matryoshka is a set of concentric rings of nodes built around each user node in order to provide trusted data storage, profile data retrieval, communication obfuscation and anonymization through indirection. A lookup service is provided in the P2P architecture to find entry-points for matryoshkas, using pseudonyms provided by the trusted identification system. *Architectural Services* in Safebook are decentralized in essence, using the "matryoshka" structure, in which users form a P2P overlay network and cooperate to provide SNS services. Thus, users can directly search, communicate and retrieve information, using the resources of their neighbours instead of a centralized service provider. *Storage* is

provided by the matryoshka overlay, in which users store their own profiles. The social links between direct friends are then used to increase profile availability. This leads to protected and public data replication across direct friends. In spite of that, data suppression is not mentioned in the public specifications of Safebook.

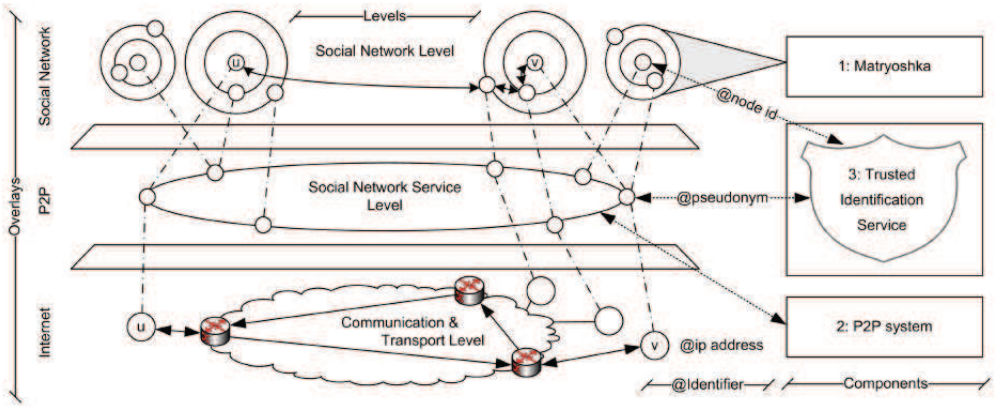

Figure 2.3 – Safebook's architecture

- PeerSoN: PeerSoN is based on direct communications between peers by using an external P2P infrastructure, called OpenDHT [BSVD09, Sch08]. In this sense, the OpenDHT overlay can be seen as a set of super-peers, providing lookup services and maintaining profile information in a distributed hash table (DHT). Peers become friends by directly exchanging content. Each peer can decide to become a super-peer or not. If a peer decides to become a super-peer it has to maintain a list of peer IDs. The services provided by the super-peers are used to locate the peer in charge of a given piece of data, and to directly communicate with this peer to retrieve the data. *Architectural Services* in PeerSoN have inherent decentralized properties for retrieval and communication. These properties are based on direct content exchange among peers, and communication between peers are performed directly when they are online. Search for peers or files are decentralized since peers request information to the OpenDHT, consisting of super-peer to provide lookup metadata. Then, the OpenDHT sends to the peers the requested information. *Storage* and data availability in PeerSoN occurs in a decentralized fashion, since each user stores her own data, and the OpenDHT is used to store metadata. Data that are encrypted (protected) are replicated in random peers, but data suppression is not mentioned in PeerSoN.

- SuperNova: SuperNova is a SNS that focuses on data availability, based on three main components: peers, super-peers and storekeepers [SD12]. Each peer can decide to become a super-peer or a storekeeper. While super-peers provide data storage and lookup services to peers that do not have enough friends in the SNS, storekeepers offer the same features but only for friends. Each peer can ask friends to become data storekeep-

ers, ensuring data availability when peers are offline. SuperNova also uses a number of incentives for peers, such as space for advertisement and monetization, to become a super-peer and thus facilitate new peers to join the system. *Architectural Services* provided by SuperNova rely on a decentralized architecture for searching. Decentralized super-peers maintain a list of user IDs, and help them to search other peers. After a user establish friendship in the system, communication and data retrieval are made directly by peers, in a fully decentralized manner. *Storage* in SuperNova is decentralized in super-peers and storekeepers. Storage space is mainly in peers for their personal data. Replication techniques in SuperNova use super-peers to provide available space for new users that do not have enough friends, as soon as they are added in the SNS, and Storekeepers keep replicas only for friends. Peers are able to view a list of super-peers and services they are providing (such as storage for peer data). Then, peers can decide on which component their information will be replicated in a encrypted form.

When the approach is based on P2P systems, a single point of data aggregation such as a central server or any kind of centralized control, is avoided. P2P is a good candidate for the development of SNSs that promote users' ownership over their data and the capability to store it almost anywhere (i.e., in friends' computer, in random peers, and in third-party external storage), this system also introduces many challenges and adverse properties due to the difficulty of ensuring good security properties such as encryption-based access control systems to prevent misuse or deletion of data from malicious members, the running time performance and the profile availability (e.g., when the user is offline) [BSVD09]. Another important bottleneck of P2P SNSs is related to the user's knowledge and expertise needed to set up and to perform self-management of the SNS.

2.4.3 Hybrid Systems

SNSs with hybrid architecture merge centralized and decentralized architectural services, such as search, retrieval and communication. An example of hybrid architecture is

- PrivacyWatch: PrivacyWatch is a SNS approach that focuses on the tradeoff between privacy and usability [AGH10, Ho12], consisting in three major components: the Client Privacy Manager (CPM), a centralized SNS provider, and a Mail server (see more details in Figure 2.4). Users can install the CPM in their computer's browser, which helps to set their privacy level and privacy preferences. Also, the CPM is in charge of information retrieval and inter-user communications. The SNS provider is only used to search friends, to store encrypted personal information and to manage User Privacy Policy (UPP) violations. A UPP is a XML document to specify and communicate, in an easy and flexible way, a user's privacy preferences. The Mail server is used as an auxiliary channel by the CPM to create an email account, which is used to store and to exchange keys and UPPs among users. *Architectural Services* are handled by a centralized SNS provider in PrivacyWatch, regarding the search property. Each user installs her own web server to directly retrieve information among peers and communication in a distributed form. *Storage* is performed in the Client Privacy Manager (CPM) component, on peer side. The CPM contains two databases: the XML database in the key manager module,

and a user database in the client access controller module. The XML database stores all keys of the user and her friends. Storage space is mainly in the user database, where data and UPP are kept. Replication is decentralized and occurs between two servers: the SNS provider and the Mail server. The SNS provider stores only encrypted data, whereas the Mail server stores encrypted keys and UPP. Data suppression is also under peer control in the PrivacyWatch specification.

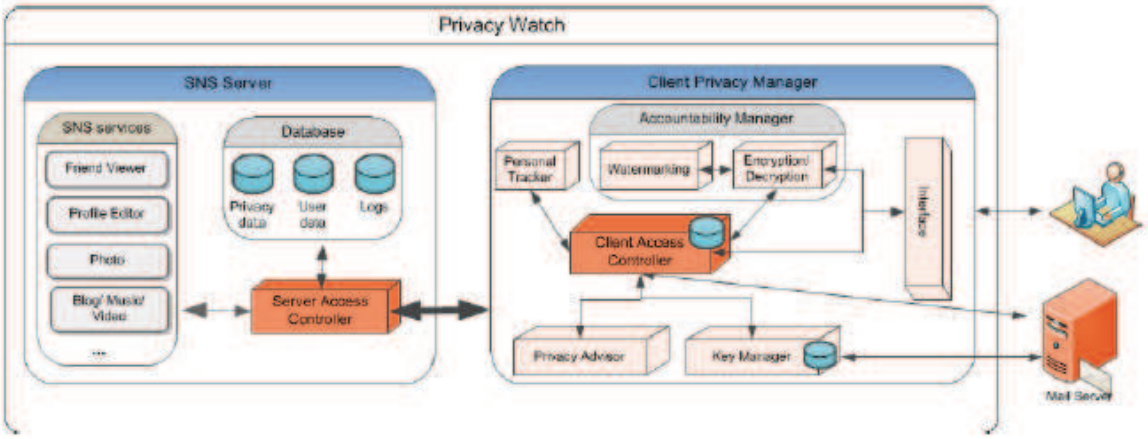

Figure 2.4 – PrivacyWatch's architecture

The approach based on hybrid architecture provides a flexible architecture to organize the main services of SNSs. This alternative provides a balance between privacy and ease-of-use, depending on the selected privacy level in the UPP. The UPP holds the user's preferences in accordance with the chosen privacy level, which determines how much information will be shared with the SNS provider. To avoid personal data disclosure, watermarking techniques are then used in the SNS to partially monitor the dissemination of information. However, there is no guarantee that the user's personal data will be safe from disclosure, which constitutes the main shortcoming in PrivacyWatch: the lack of the UPP's automated enforcement. This type of hybrid architecture allows the choice of centralizing the search functionality, and to distribute retrieval and communication functionalities, even though other possibilities could be used. Further discussions about possible SNS design options will be discussed in chapter 4.

2.4.4 Discussion about Decentralized SNSs

The three categories of decentralized SNS solutions previously presented rely on the assumption that keeping data within users' devices protects against abuses from the SNS provider. These proposed architectures are built on the principles of PbD (section 1.6) with a focus on user-centric foundations and privacy by default settings. In a general sense, decentralized SNSs may provide better control to foster freedom of speech, autonomy, and privacy of user data.

When discussing decentralized architectures, technological and societal factors should be taken into account. Important advantages of decentralized approaches, according to Baran [Bar64], are their high resilience against disruptions and their effectiveness in repairing topological damages from redundant connections. Moreover, avoiding data analysis of personal information (for advertising purpose, for instance) may lead to a better protection of users' privacy.

A well-designed decentralized SNS should be able to provide similar functionalities and usage experience compared to existing centralized SNSs. However, decentralized approaches may have some limitations when compared to centralized SNSs. Narayanan et al. [NTB+12] identify several difficulties in their elaboration and, despite much work and many different efforts, these systems have tough barriers towards their adoption. The first issue in decentralized SNSs is related to technical factors that are harder to be designed if compared to centralized systems, such as fraud and spam detection, or search. Another issue is the economic feasibility. Indeed, decentralization requires standardisation and sustainability without potential monetization, since the majority of the users are unwilling to pay. Since users' data are kept as much as possible on their own personal devices, limitations such as bandwidth issues and restricted connectivity may occur. Moreover, a better technical expertise from users to manage and configure the system is required, such as software installations and inevitable personal decisions, which can lead to cognitive overload.

Some recommendations for developers of decentralized SNSs to improve user's experience and business practices are [NTB+12]: consideration of the economic feasibility of the SNS design, evaluation of what features and benefits users need or want, incorporation of other advantages besides privacy and socio-legal choices, the design of SNSs with standardization, target limited set of features for a minimum viable product, and compliance with privacy regulations to achieve a balanced SNS.

The current SNS categorization in decentralized (including their sub-categories: networks of trusted server, P2P SNS, and hybrid systems) and centralized is simple and practical. Nonetheless, the existing categorization is insufficient because most systems in the P2P SNS category could also be considered as hybrid, should the priority be given to another functionality, such as search. Therefore, a more fine-grained classification should be established, possibly leading to a better understanding of the implications of individual design choices. To bridge this gap, a classification improvement proposal will be presented in chapter 4.

2.5 Conclusion

Over time, SNSs have grown in features and are widespread adopted around the world. Centralized SNSs are widely used, due to the fact that they fit users' needs, allowing people to share information and to access many services and applications. However, centralized SNSs hold massive amount of users' personal data in a single administrative domains leading to prominent privacy risks.

The limitations posed by centralized SNSs have motivated the development of decentralized alternatives. Decentralized SNSs are a promising approach to develop systems and

contribute to data sovereignty[8] and capture the multidimensional concept of privacy, where users keep control over data upon collection, use and dissemination. Beyond the surveillance of the server provider, decentralized SNSs have the potential to reach power balance, opening opportunities to innovation, and empowering users' democratic participation. While there have been advances on the development of decentralized SNSs, risks should be carefully discussed and the prioritization of design choices established. Also, developers should be aware of the challenges introduced by decentralization, such as data availability, security, performance, user acceptance, and scale.

It is worth noting that all major limitations and problems discussed about centralized SNSs will ultimately lead to privacy problems. Therefore, the main challenge is to maintain control over personal data in the SNS context, preventing the users' privacy violation. The current researches aiming to mitigate privacy problems and limitations will be described in the next chapter.

[8]Data sovereignty is the concept that an individual is able to control the processing of personal data [AGH10].

Chapter 3

Privacy in SNSs

The popular use of SNSs for online messaging and information exchange has made available online massive amount of personal data. In general, social interactions require information sharing between the involved parties, which implies knowing with whom, and to which extent the information is shared. The shared information leads to many concerns about data privacy, mainly due to the fact that the distinction between personal information and general content diminishes further within the SNSs [LHB+14]: on the one hand, users have a wide range of new possibilities for sharing and creating digital content within their own webspace in the SNS, which is separated from other users; on the other hand, the users' control over their own information is weak due to the SNS capabilities such as wall posts, comments and tagging of photos.

Recent events show that a wide range of personal information often leaks and several legal cases and complaints[1] have raised questions in terms of control of private information. Following the baselines from previous chapters 1 and 2, the present chapter will extend and explore the SNS context under the lens of privacy protection.

This chapter is organized as follows. Section 3.1 describes privacy issues and identifies the main threats to privacy in SNSs. Section 3.2 examines how privacy policy are defined and managed in SNSs. Section 3.3 discusses the application of privacy regulations to SNSs. Finally, some conclusions of this chapter are presented in section 3.4.

3.1 Privacy Issues in SNSs

The essential feature of a SNS is the creation of user profiles and their social relationships. Within SNSs, users can communicate with each other, share and exchange information. As a consequence, the large amount of data about themselves and their social relationships, such as uploaded content and social graph, are saved into the SNS.

[1] http://europe-v-facebook.org/EN/en.html

Privacy concerns have emerged about potential abuses or losses of personal information of users. The first need for privacy comes from the user's desire to control what she shares with other users, since sharing content gradually became easier, faster and more direct [EB13]. However, privacy issues in SNSs are also related to the social graph. Indeed, knowing the social relationships of a user may lead to serious damages to her privacy. For instance, the Gaydar project[2] demonstrates the possibility to predict a user's sexual orientation based on her online friends.

More generally, SNS threats on users' privacy are extensively reported. Ho [Ho12] classifies privacy threats into three categories: security (e.g., identity theft, profile cloning, phishing, cyber predation), reputation and credibility (e.g., employees being fired due to social media exposure) and profiling (e.g., spam, unsolicited collection of user's data). Privacy threats may come from many entities in SNSs [CMS09, ZSZF10]:

- Malicious authenticated users;
- Malicious third-party application providers;
- Malicious authoritative entities.

In the next subsections, the attacker's capabilities with respect to privacy threats is characterized depending on the SNS design and architecture (i.e., centralized or decentralized).

3.1.1 Malicious Authenticated User

A malicious authenticated user has similar capabilities in centralized and decentralized SNSs, and can adversely affect the privacy of users in different ways. Concerning the privacy threats of the "security" type, a malicious authenticated user can either steal the identity of a user (identity theft), or impersonate the user (profile cloning), or simply become a friend by pretending to have the same centers of interest that the user (cyber predation). A malicious authenticated user may perform identity theft by acquiring the credentials of the user (e.g., by stealing the password of the user, possibly through phishing) and acting on her behalf with full access to profile, relations and communication traces [CMS10]. A malicious authenticated user can also clone the profile of a given user so as to fool the friends of this user. Profile cloning occurs because users often set their profiles public. But even when access to a user profile is restricted to "friends only", in Facebook for instance, the restriction can possibly be easily bypassed through tagging, such that "friends of friends" can also access the information [Deb11]. When the malicious authenticated user has obtained the profile information, she can subsequently create a fake profile. After cloning the victim account, the malicious authenticated user can send fake requests to the friends of the victim user. This privacy violation is based primarily on design issues, which could be improved by the deployment of tools, like iCloner to detect similarities between profiles [BSBK09]. Similarly, a malicious authenticated user can simply create a fake profile pretending to have some specific information and then send fake requests to others users. Such an action is often successful

[2] http://journals.uic.edu/ojs/index.php/fm/article/view/2611/2302

since many users tend to accept friend requests even if they do not know the user that sends the request.

The privacy threats coming from malicious authenticated users can also cover profiling. Indeed, by using public information such as those of the user profile, possibly including the list of the user's friends, a malicious authenticated user can try to infer personal information. Such a threat is even worse when the malicious authenticated user exploits the social links, such as the friend-of-friends relationship. Indeed, friends have more knowledge about each other, allowing them to infer more private information. Especially, in decentralized SNSs, user data are often stored encrypted on friends' devices, but Greschbach et al. [GKB12] pointed out that friends of a user can use metadata (e.g., how much disk space the information takes, how often a specific node requests similar data at a specific time of the day) as well as traffic information (e.g., requests for particular pieces of information) to infer personal information without decrypting the stored data.

Finally, a malicious authenticated user can defame other users, causing serious reputation problems [AGH09]. Such a threat is even worse when the malicious authenticated user first steals the identity of the user or impersonates her.

3.1.2 Malicious Third-party Application Providers

In centralized SNSs, the main privacy threat related to a malicious third-party application providers is the profiling of users. As discussed in section 2.3.1, centralized SNSs are a central place for business based on economic models where revenue depend on information about users. Typically, in a rich SNS like Facebook, third-party application providers (e.g., quizzes and games) may sign a contract with the SNS provider specifying the users information it can have access to. Such a contract often does not specify the purposes of this collection. Besides, the common strategy adopted by centralized SNSs is an "all or nothing" policy [CPS13]: when a user installs a third-party application, she can only agree that the application provider has access to her information, such as her profile or the list of her friends, but she can not limit this access. Krishnamurthy and Wills [KW09] show in a study that most users in centralized SNSs are vulnerable to leakage of their SNS identity information to third-party application providers. The study used 12 different SNSs (Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LiveJournal, MySpace, Orkut, Twitter, Xanga and LinkedIn) with distinct degrees of personal information availability, and conclude that photos, locations, genders and names are widely available and thus prone to leakage, while email addresses, zip codes, phone numbers and street addresses are rarely available and have less chances of leaking. By using the collected information about the users, a malicious third-party application provider can infer personal information. Notice that, to mitigate the leakage of users' information to third-parties, some recent changes in Facebook application policies allow users to interact anonymously with third-parties and also to decide what information the user wants to reveal[3].

Beside the profiling of users, a malicious third-party application provider in a centralized SNS can also steal security information such as passwords or banking data. Indeed,

[3] http://www.forbes.com/sites/larrymagid/2014/05/22/facebook-changes-default-privacy-setting-for-new-users/

the applications may contain malicious code designed to perform classical attacks such as phishing.

Existing decentralized SNSs do not provide third-party applications, and the challenge remains in determining how third-party applications could be integrated into decentralized SNSs. However, we can reasonably assert that if third-party applications were to be integrated, malicious third-party application providers would have less capacities in decentralized SNSs than in centralized SNSs. Indeed, since the SNS functionalities are provided by a set of entities, it will be harder to track users' online activities, thus limiting the capability of user profiling. Besides, distributing both the control of the infrastructure and the management of user's information among peers would help to mitigate risks of malicious third-party application providers. However, as in centralized SNSs, a malicious third-party application provider of a decentralized SNS could be able to include malicious code into applications so as to perform classical attacks such as phishing and to steal security information such as passwords or banking data.

3.1.3 Malicious Authoritative Entity

A malicious authoritative entity has more capabilities in centralized than in decentralized SNSs. In centralized SNSs, the only authoritative entity is usually the SNS provider. Therefore, since it has full access to all users' information and to the network resources [BKW09, CMS09, CMS10, GKB12], a malicious SNS provider has very strong capabilities. Indeed, since the SNS provider is in charge of SNS functionalities, and data storage, information monitoring, aggregation, and direct or indirect collection of data can easily be performed by a malicious SNS provider, allowing to steal security information such as passwords or banking data, but also to perform profiling. A malicious SNS provider can also simply requests personal information from the users in order to access SNS services. More generally, malicious SNS providers have been known to perform several types of attacks including face recognition, secondary data collection and data retention [PB13], profiling and censorship [CMS09], massive targeting advertisement, and behavior analysis [BSVD09], but also to sell their users' personal information and social graph connections [BJE+10].

In decentralized SNSs, there is not only one authoritative entity since the SNS services are provided by a set of entities that collaborate among them. Thus, a malicious authoritative entity has less capabilities than in centralized SNSs. In particular, a malicious authoritative entity can not access users data (i.e., users profile or even friend relationship) without the collaboration of the other authoritative entities.

3.1.4 Privacy-enhanced SNSs

As presented in the previous subsections, both centralized and decentralized SNSs are vulnerable to various kinds of attacks. This has led to define the notion of *Privacy-enhanced SNS (PSNS)*, that characterizes privacy in SNSs into three properties [AGH10, Ho12]:

1. *Privacy awareness and customization:* a PSNS should makes the user aware of potential risks of sharing information with other people. In addition, it should also provide an easy and flexible way for users to express their privacy concerns in terms of a personal

policy, and to compare it with the privacy policies of other entities such as the SNS provider, applications or other users;

2. *Data minimization:* a PSNS should collect only personal data that is strictly needed. A user should be able to check whether her information is accessed by the SNS provider or by third-party application providers, and how this information is used. In particular, the SNS services have to clearly state which personal information is needed from users and how it will be processed. In Aïmeur et al. [AGH10], a functional prototype was introduced to allow a user to make her decision on whether she accepts or not the SNS services. The PSNS should have an built-in mechanism to control and limit access to information as previously authorized by the user;

3. *Data sovereignty:* it should be explicitly stated in the privacy policy that a user's personal data belongs to her and not to the SNS provider. For instance, the SNS provider should not use personal data without explicit consent and should not be able to sell it to other entities. Moreover, if the user decides to quit the SNS, the SNS provider should explicitly delete all user's stored information. A user should also have the possibility to track how her information is disseminated but also to control personal information related to her and posted by other users (e.g., a tag on a picture that points to her profile).

Privacy awareness is an important property that encompasses the perception of which personal information other parties have received and how this information is processed. Users are typically informed on how SNS providers handle user's personal data by the means of a privacy policy provided by the system [AER02]. Data minimization is one of the main principles to limit the collection of personal information, and data sovereignty provides the elements for users' control over personal private information flow, including the option to decide what personal information can be collected. The notion of PSNS is ultimately operationalized through the definition of a privacy policy.

The previous analysis shown that privacy threats are greater in centralized SNSs than in decentralized SNSs. In particular, the most significant privacy threat in centralized SNSs come from a malicious SNS provider, because the client-server architecture requires that all information and communication from all users within the SNS flows through central servers operated by the SNS provider.

Of course, the issue of malicious SNS providers could be addressed through the enrichment of the existing centralized SNSs by incorporating security and PETs mechanisms. For instance, some privacy plugins have been integrated within existing centralized SNSs, in order to hide content to the SNS provider using cryptography (i.e., NYOB [GTF08], Persona [BBS+09], Lockr [TSGW09], amongst others). However, some aspects related to the design of centralized SNSs clearly are against the privacy of the users (e.g., traffic analysis from the SNS provider is facilitated by the centralized design).

Conversely, in decentralized SNSs, by avoiding a single central authority and consequently promoting more decentralization of data and services among users, the level of privacy is enhanced. Therefore, it is important to consider privacy related issues on the SNS design and architecture at several levels. However, it is not clear how to provide a complete set

of properties for SNSs since privacy is impacted by many design choices. Design challenges at several levels in terms of privacy protection on the one hand, and availability, security and management on the other hand, should be compared and evaluated in systematic ways towards the development of privacy-aware SNSs. In order to properly analyze risks according to different degrees of decentralization in SNSs, the chapter 4 describes the first contribution of this thesis: a multi-criteria analysis grid based on degrees of decentralization for SNSs design, that is useful in a privacy by design methodology to compare and classify SNSs based on their design approaches.

3.2 Privacy Policy Management

Privacy policy management is a valuable tool for privacy protection, enabling users to avoid or minimize the collection and use of personal data by others. It ensures that personal and private data are managed with respect to the privacy policies, which are commonly used to represent and describe privacy regulations in terms of permissions over usage of personal data, and obligations to be fulfilled.

A lot of empirical research has been made in the last years, showing how users perceive privacy and information disclosure in SNSs. Aïmeur et al. [AGH09] show that users have different privacy expectations with respect to each piece of personal data. A similar result is expressed by Karyda and Kokolakis [KK07], where different groups of users have different perceptions of privacy concerns in a variety of degrees and methods to protect it. Depending on the perception and awareness of privacy problems related to SNS usage, users can better customize privacy policies.

The next subsections are organized as follows. Subsection 3.2.1 explains privacy settings in existing SNSs. Subsection 3.2.2 states similarities and difference between access control policies and privacy policies. Subsection 3.2.3 presents the major privacy policy languages. Subsection 3.2.4 describes privacy policies in SNSs to indicate two different contexts, users policies and system policies. Subsection 3.2.6 defines the architectures to evaluate privacy policies.

3.2.1 Privacy Settings in Existing SNSs

The majority of SNSs provide privacy control settings to protect users from undesirable use of personal information, which often require to set the visibility and the accessibility to others. Typically, SNSs let users grant privileges to different entities (e.g., user's friends, all users, friends of friends). Thus, users post information about themselves and specify the people with whom the information can be shared. However, these settings usually do not contain options to hide information from the SNS provider.

The specification of privacy policies can be used to regulate how much information is allowed to be shared and who is allowed to know the information. Often, these privacy policies are referenced and used in SNSs in the form of access control policies. Typically, these policies have been expressed and managed in a centralized manner: a single entity manages and enforces the policies of the whole system [DCdVS06]. In centralized SNSs, users are usually allowed to define their own privacy settings through access control policies

over their resources for privacy protection [AGR14]. These access control policies focus on transitive access control, which is the ability to extend the list of authorized users that have access to an information [Gür10]. In particular, a user may have control over the visibility of her contact lists, her own profile information, and her own uploaded or posted content. However, transitive relationships allow to extend the visibility of personal information. For instance, if a piece of information is accessible to friends of friends, then friends of the user co-determine who is allowed to access that information by defining their own set of friends.

Privacy settings have a range of options, depending on the SNS features. For instance, MySpace only allows users to limit who can access their page, but by default everyone has access to all available information. LinkedIn allows users to change the visibility of their profiles (i.e., the profile can be hidden or visible to other users) and select who can see their activity feed. Google+ allows users to customize their circles of friends according to trust relationships. In Twitter, while users can follow and thereby view the tweets of any public account without prior approval, for private profiles the approval to be "follower" and thus view the tweets is necessary. Moreover, tweets that are assigned to be public always remain public, no matter whether account status is changed to private afterwards [XV09]. Facebook settings allow users to control who can search them, how they can be contacted, as well as what posts and data are published or hidden. Over time, a number of re-designs in Facebook default settings has been made towards high accessibility by default[4].

Although people wish to decide what kind of information they share, and privacy settings are intended to assist users on how information will be presented and accessed by others, privacy controls of SNSs may not adequately reflect the use of personal data [ARG11]. In a study using 16 different SNSs (Facebook, MySpace, LiveJournal, Bebo, Hyves, Friendster, Hi5, Tagged, Netlog, Badoo, Nexopia, Perfspot, Twitter, LinkedIn, Orkut, LiveSpace), Anthonysamy et al. [AGR13] revealed that only 23% of privacy policy statements in textual form have a mapping with the corresponding runtime implementation of privacy settings. This is one of the reasons why privacy is currently a major concern among SNS users and highlights the insufficient state of privacy management.

Regarding decentralized SNSs, each user define privacy rules in the form of access control policies according to the type of relationship or trust. Then, users set access policies to their data, and often encryption techniques are also used, to ensure that only users possessing a key are authorised to access the data. For instance, in SafeBook, all attributes of a user's profile can be set with particular access control policies and published data can be categorized as private, protected or public: in the first case (private) the data are not published, in the second (protected) data are published and encrypted, and in the last case (public) data are published without encryption. A similar strategy is used in PeerSoN, where access privileges to user's encrypted data are accessible through the distribution of keys between friends. In SuperNova, the user data are also divided in public, protected and private. Public data can be accessed by any user in the network. Friends can access public and protected data whereas private data are only for the user herself. In addition, data at super-peer are stored in encrypted form. In Diaspora, types of data such as name, current profile picture, Diaspora ID and public posts are considered public. Private data are the full profile, private messages

[4]http://mattmckeon.com/facebook-privacy

and contact lists. Data encryption is based on groups according to three levels: none, low, high. In the first case, there is no encryption; in low level the encryption is made by the server; and finally, in high level data are encrypted by the user. In FOAF, users specify AIR[5]-based access control to restrict access to resources. Finally, in PrivacyWatch [AGH09], the access matrix depends on the privacy levels (no, soft, hard and full) and on different groups (best friends, normal friends, casual friends and visitors). In this matrix, each piece of data of the profile can be characterized as poisonous, harmful, harmless or healthy. As a result, [AGH09] proposed to relate these privacy levels with the amount of the information that should be encrypted. The default recommended setting for the "no" privacy level is to not encrypt data, "soft" privacy level suggests to encrypt poisonous data, "hard" privacy level suggests to encrypt poisonous and harmful data, and "full" privacy level suggests to encrypt all data.

3.2.2 Access Control Policies and Privacy Policies

It happens that access control policies, as used by most SNSs, are inadequate to protect privacy in SNSs [KA10]. More specifically, as pointed out by Ni et al. [NBL08], access control policies and privacy policies are different by definition: the former are widely used for controlling access to personal information and valuable resources in various environments, whereas the latter are specifically designed to protect privacy when collecting, using, and disclosing personal information. For this reason, privacy policies are a more expressive and efficient way to represent user privacy preferences, and access control policies are a special case of these policies.

In general, policies can be written in human readable format or in computer readable format. These policies can be found in different forms and contexts, establishing rules to govern how the information should be handled, enabling control and ensuring privacy. However, using a formal specification for describing the policies allows to reason about their consistency, as well as to compare policies.

- **Access Control Policies**

  According to Bertino et al. [BBC+09], access control policies determine who is authorized to access what data or resources and under what circumstances in a computer system. An access control policy rule [BBC+09] is a tuple of

  $$< Subject, Action, Resource, Purpose(opt.), Condition(opt.) >$$

  where *subject* identify a subset of entities that request access to a resource, *action* is any operation (e.g., read, write) that can be applied to a resource, *resource* identify an information for which access can be restricted, *purpose* is an optional argument selected from a predefined set of purposes for executing an action, and *condition* is an optional boolean expression to express environmental properties, in order to define more fine-grained policies.

[5]Policy language for dependency tracking based on a production-rule system.

- **Privacy Policies**

  Yee and Korba [YK05] provide a privacy policy specification that uses the CSAC (section 1.3.2) and the Directive 95/46/EC (section 1.3.3). The elements composing their privacy rules are

  $$< Collector, What, Purpose, RetentionTime, DiscloseTo >$$

  where a *collector* is the user who wants to collect the information, *what* is the nature of the information, *purpose* states the reason why the information is being collected, *retention time* relates to the amount of time the information is kept, and *disclosure to* are the parties to whom the information can be disclosed. This privacy policy specification covers standard cases for privacy policies. However, privacy policies that require more complicated rules bring the need for *Condition* and *Obligation* elements [KSW03]. In fact, by using the condition element, complex environment constraints may be imposed on a privacy rule, and obligation element defines actions that need to be performed after the user request is fulfilled (e.g., A doctor is allowed to write in a patient's medical records for treatment, whenever this action is performed, the patient must be notified.). Based on this observation and the simple privacy rules from Yee and Korba [YK05], in this thesis the following extended privacy policy is considered:

  $$< Collector, What, Purpose, RetentionTime, DiscloseTo, Condition, Obligation >$$

Overall, classical components of access control policies are *subjects*, *actions* and *resources*, while *purpose* is an optional feature [BBC+09]. Nonetheless, for Ashley [Ash04], *purpose* is an indispensable attribute of a privacy policy and a feature that separates it from a traditional access control policies. Indeed, *purpose* takes the major role in personal data protection: within the E.U. Directive 95/46/EC, the principles of finality and proportionality (see section 1.3.3) are strongly connected with *purpose* since the nature of the provided information must be only what is strictly necessary.

As shown in the previous subsection, major approaches to protect users in centralized or decentralized SNSs focus on access control policies more than privacy policies, current SNS policy specification can be analysed by considering the triplet of components (**Purpose, Disclose to**, and **Retention time**). Table 3.1 illustrates a qualitative analysis, including the following scale:

- *Unknown (?)* means that there is no available information about this element in the SNS specification;
- *Existent (+)* means the availability and existence of the privacy policy element;
- *Nonexistent (0)* means that the privacy policy component is explicitly not addressed or not implemented in the SNS.

Table 3.1 – Privacy policy elements in SNSs

	Facebook	*SuperNova*	*Diaspora*	*PrivacyWatch*	*PeerSoN*	*Safebook*	*FOAF*
	? + 0	? + 0	? + 0	? + 0	? + 0	? + 0	? + 0
Privacy Policy Elements							
Purpose	?	0	0	0	0	0	0
Disclose to	?	0	0	+	0	0	0
Retention Time	?	0	0	0	0	0	0

Despite the fact the notion of *purpose* implies transparency for the use of information, none of these approaches has mentioned this key element. The same happens with *retention time*.

The element *disclose to* appears in only one approach. For example, in Diaspora's privacy policy, there is a topic called "controlling personal information" (no selling, distributing or leasing personal information to third-parties unless user permission). In PrivacyWatch, the UPP contains the element "access-rights" indicating how the information should be handled using values such as "no distribution".

3.2.3 Privacy Policy Languages

There are various alternative languages to represent privacy policies. These privacy languages can be developed by using either rule-based models such as P3P, XACML, and EPAL, or logic-based models. A rule-based model states a policy as a set of rules, whereas a logic-based model states a policy in terms of formulas in an appropriate logic, such as first-order logic, first-order linear temporal logic [AD07], or deontic logic [PD10].

- *P3P*

  P3P is a declarative language developed by the World Wide Web Consortium (W3C) to communicate privacy policies adopted by the website and to give users the possibility to assess whether these privacy settings are acceptable [Con06]. A service provider can define a P3P policy, which is an XML document describing the name and contact information of the website (*entity* element), the information that may be collected (*categories* element), how information may be used (*purpose* element) and shared (*recipient* element), whether and how individuals can find out what personal data websites keeps about them (*access* element), the retention period (*retention* element), and options for dispute resolution (*disputes* element). The policy specification statements based on P3P are of the form [Ash04]:

  Allow a [user] to [use] [personal data] for [purposes] under [condition, consent]

  A user is able to specify her privacy preferences in the terms of a policy language like APPEL [Con02] and, before communicating personal data to the service

provider, her P3P agent[6] compares her privacy policy with the service provider policy to verify whether they are compatible or not.

- *XACML*

  XACML is a policy language mainly used for expressing access control [Org14]. The XACML structure is composed by three components: policy set, policy, and rules. A policy set can cover one or many policies, where each policy is a set of access control rules. A rule includes a target (describing the subject, action and resource), a rule effect (allow or deny), and an optional set of obligations. The last version of XACML has two purpose attributes defined in the privacy profile specification: the first is the "resource:purpose", which defines the purpose for which the data resource was collected, and the latter is the "action:purpose", which indicates the purpose for which access to the data resource is requested.

- *EPAL*

  EPAL is a formal language developed by IBM, based on its academic abstract language E-P3P [AHKS02] and designed to enable organizations to translate their internal privacy policies into an XML-based computer language. The EPAL privacy policy model consists in an EPAL vocabulary and a set of EPAL privacy policies rules. The vocabulary defines the terms to be used within the policy, in the form of a six-tuple: users, data, purposes, actions, conditions and obligations. The privacy policy is a five-tuple: the vocabulary, a ruleset using the vocabulary, the global condition, a default ruling, and a default obligation. An EPAL policy is expressed in a flat structure, which contains a set of privacy authorization rules that allow or deny requests [BPS03]. Then, the access decision is based on the purpose component. The policy specification statements based on EPAL are of the form [BDS04]:

  A [user] should be [allowed or denied] ability to perform an [action] on [data] for [purpose] under [condition], yielding an [obligation]

  EPAL policies are machine enforceable, where an authorization engine parses EPAL policies to generate a ruling for each request, and subsequently an enforcing system will execute the ruling [AHKS02, QCQ$^+$12].

- *Logic-based languages*

  In addition to the XML-based semi-structured models, it is also possible to design logic-based languages for privacy policies. In particular, many kinds of deontic logics [von51] (i.e., which embed the notions of obligation, interdiction and permission) and temporal logics [Pri67] have brought new perspectives in the domain of privacy policies. Such models have been used for general security policies [Ort96], complex access control policies [CCBS05], information flow control policies [Cup93] or specifically for privacy and personal data protection frameworks [PD10, ABvdT10]. Similarly, Contextual

[6] A P3P agent is a software tool used on the client side to interpret a site's P3P policies.

Integrity (CI) is a normative model and logical framework for expressing notions of privacy in legislations and reasoning about the flow of personal information [BDMN06]. The CI approach is based on positive and negative temporal logic formulas to capture the transmission of data between users. Another example is SecPAL for Privacy (S4P), a generic logic-based privacy language to express user preferences and service policies [BMB10]. The S4P syntax uses two modal verbs, "may" and "will", which allow service privacy policies to express which possible behaviour of the service (called may-query), and which service promises can be executed with the user's personal data (called will-assertion). Also, S4P specifies a user preference policy to state permission in which service may or may not be executed with her personal data (called may-assertion), and obligation that a service must exhibit (called will-query). Contrary to these duality regarding policy specification, SIMple Privacy Language (SIMPL) is a more concrete language allowing data subjects and data controllers to express both preferences and policies using a friendly interface [Mét09, MM09]. SIMPL provides formal guarantees that a developed system complies with the specified semantics of a privacy policy.

Despite significant efforts towards the adoption of P3P, this language suffers from some shortcomings. The P3P syntax has predefined types of data and no obligation in the rules, which might not be expressive enough. The only operation supported by P3P on data is "use", but it does not define a set of operations on data such as read, write, create or delete [Ash04]. Besides, the main problem is the lack of automated enforcement and auditability in websites, because of the declarative nature of P3P. Users are unable to check if the expressed privacy policy is actually enforced by a web service.

In XACML, complex syntax and semantics make policies difficult to write. XACML policies syntax generates long and complex policies, which are often verbose and thus prone to errors [LPL+03]. Moreover, the purpose attribute is not required either for data collecting in the "resource data" category or data accessing in the "action data" category. EPAL is similar to XACML to some extent, but the main difference is that EPAL is specifically targeted for privacy policies, while XACML deals primarily with access control policies .

The advantage of the logic-based approach to privacy languages is that it ingrains reasoning tools, facilitating the enforcement techniques themselves. The main drawback is the computational tractability of these reasoning procedures in a domain where PSPACE-completeness is often a lower bound [Rey03]. However, even though these models offer expressivity in their semantics of usual privacy regulations, they are still in a high-level of abstraction.

There are some proposals, in various level of maturity, for representing privacy policies in SNSs based on relationships among users. Those relationship-based models are inspired by the intuitive idea that the social relationships of users can better define who is authorized to access their information. In this context, some approaches have been developed by using access rules for social relationships. For instance, Carminati et al. [CFP09] describe a relationship model that allows a user to specify access policies associated with a level of trust corresponding to a type of relationship (friend of, colleague of, etc.). A more formal algebraic model for relationship-based access control, implemented in Facebook, is proposed by Fong et al. [FAZ09]. The social graph in this algebraic model is used to extract the topological

information used to formulate policies, such as degree of separation, known quantity, clique, etc. Following this paradigm, relationship-based policies can also be formally represented using logic. For instance, Fong [Fon11] proposes a policy language based on modal logic for supporting the specification and composition of policies. He formulates a relationship-based access control model for social computing applications. Recently, Pardo and Schneider [PS14] proposed a privacy policy framework for SNSs that enables reasoning about epistemic and deontic assumptions. This framework consists of a formal model of the SNS, the syntax and semantics of a knowledge-based logic, and a formal language to describe privacy policy. This knowledge-based logic allows to express the distributed knowledge of an information, which is known by the whole group. Moreover, this privacy policy language permits a user to define policies over other users' resources based on the knowledge mentioned above. The specification of many privacy policies over the same content is a very desirable capability because it allows users to perform their rights to control content associated to them, even though eventually generating conflicts of interest caused by contradictory preference policies. The major focus of this framework is reasoning about the general knowledge of the users, and not on how handle inconsistency when multiple users specify privacy policies over the same content.

Finally, it should be noticed that in SNSs, where many users can be affected by content disclosure, privacy protection mechanisms are needed to enforce the privacy of all involved users, specially when dealing with information related to other users, besides the data publisher. In this context, policy-based approaches allow the access request decision based on the relationship between the data publisher and the requester. Nevertheless, the majority of the approaches are limited since the shared data may be associated with other users besides the data publisher and the requester. Consequently, a mechanism for joint policy enforcement of multiple users privacy policies for the shared data has to be properly designed, considering and respecting the privacy preferences of all involved users.

3.2.4 User Privacy Policy vs. Service Provider Privacy Policy

Privacy policies allow to specify what information can be collected, how it can be used, and with whom it can be shared. These policies are also meant to inform users of the choices they have regarding the management of their personal information, such as sharing with third-parties or removal of a specific content [KBCR09]. SNS providers and users are linked to different points of view and understandings, leading to major issues in relation to the existing privacy policies.

- **The user side**

  Privacy policies on SNSs are very rich and heterogeneous because users have distinct privacy preferences. In this regards, SNSs usually allow every user to declare their privacy preferences through *user policies*. On the one hand, these policies among users are often implemented in SNSs as access control policies, resulting in restrictions over data depending on the type of relationship users have with each other within the SNS. For instance, a user can determine who can access her profile and friends list, or read and write messages. On the other hand, existing centralized SNSs do not have fine-

grained policies. For example, Facebook does not allow a user to hide portions of their relationships with friends. On the opposite, the specification of personal user privacy policies is proposed in PrivacyWatch [Ho12] through the concept of UPP, which is expressed in XML format including the following elements: policy, owner, receiver, and access-rights. By using a UPP, the user is able to identify who can access her data, which kind of data is being accessed, how her data will be used, and determine what kind of tracking is allowed.

While these policies aim at enabling users to share information at various levels of granularity, according to Gross and Acquisti [GA05] most users do not change the default privacy settings provided by the SNS, which tend to maximise disclosure and minimise privacy. In addition, users are often not very knowledgeable about security features [AG06]. Consequently, in spite of privacy controls, 55-90% of users in SNSs retain default settings for the viewing of profile information and 80-97% for the viewing of friends [KW09].

- **The SNS-provider side**

  Similarly to user policies, the SNS provider may also have a *system policy*. Nevertheless, these policies are not on the same level and the SNS provider may constrain user policies. Specifically, there is usually no access control policy between users and the SNS provider to hide or restrict the information from the latter, allowing access to any users' data, including browsing behavior, private uploads, IP addresses, and message logs. Conceptually, an SNS privacy policy is a high-level description, written in human readable format about the organization's privacy practices, which shall contain information regarding the purposes about the processing of collected data and the rights of data subjects [GZ09].

  As an example, let us consider the privacy policy of Facebook. Recently, the term "Privacy Policy" in Facebook was replaced by the term "Data Use Policy" [Fac14], with the justification that the statement is consistent with this terminology. The term "Data Use" is more appropriate since Facebook's policy is vague and users do not have much control on how their personal data are collected, used and disseminated to others. According to Ni et al. [NBL08], privacy policies are characterized by the concepts of collecting, using and disclosing information. Inspired by this characterization, three examples from Facebook's Data Use Policy can be quoted:

  - Policy 1 (Information Collecting) - *"We receive data whenever the user visits a game, application, or website that uses Facebook platform or visits a website with a Facebook feature (such as a social plug in). This may include the date and time of the visit in the website; the web address, or URL being used; technical information about the IP address, browser and the operating system being used; and, the user's ID (if logged on to Facebook)"*. In this policy, the user does not know exactly which data are collected, even though some types of data are given in example.

– Policy 2 (Information Using) - *"We only provide data to our advertising partners after we have removed the user name or any other personally identifying information"*. Indeed, in this policy the provider determines that information is used for advertising. Conversely, Facebook does not inform for what purpose the information will be used by third-parties (third-parties should clearly state which kind of analysis they perform on the user's data and how the information will be used).

– Policy 3 (Information Disclosure) - *"When the user visits an instant personalization website (Facebook website partners), we provide to the website with user ID, the friend list, as well as age range, location and gender"*. In this policy, the SNS probably provides more information than necessary to the third-parties, which can imply a disclosure of sensitive information of the user.

Other examples can be found in the privacy statement from Google+'s privacy policy [AGR14]:

– Policy 1 (Information Using and Disclosure) - *"We may combine personal information from one service with information, including personal information, from other Google services - for example to make it easier to share things with people you know."* In this policy, there is lack of precision in describing what constitutes personal information, across which services and how.

– Policy 2 (Information Collecting) - *"We may use information that you tell us about yourself to personalize ads on search"*. In this policy, the SNS used generalised terminologies in describing the data item that will be used for personalisation purposes.

Although these policies are legible and written in natural language, the user may have difficulties understanding it since they are long and imprecise. For example, studies have revealed that few users actually read privacy policies, and only a few users do understand the content since it generally requires college-level reading skills [Cra03]. Additionally, the service provider may present privacy policies which do not adequately reflect its privacy practices on users' personal information [ARG11, AGR14].

Among all decentralized approaches analyzed in section 2.4, Diaspora[7] privacy policy was written in human readable format and PrivacyWatch uses the UPP, which is a machine-readable formalism to describe the user policy, whereas the other SNSs analyzed (e.g., SuperNova, PeerSoN, Safebook and FOAF) do not mention their system privacy policies.

Regarding Diaspora, the system is composed by 129 PoDs. Some of them, such as diaspora.eu, comply with the textual privacy policy statement, whereas others, such as the largest Diaspora server (joindiaspora.com), do not even mention their privacy policy terms. Although *diaspora.eu* does have statements, they still have vague terms and do not describe how data is collected and used. Examples are:

[7] https://diasp.eu

- Policy 1 (Information Using and Collecting) - *"Cookies help us to provide you with a better website by enabling us to monitor which pages you find useful and which you do not."* This policy mentions the passive information monitoring and aggregation operation performed by the SNS provider, but do not determine the kind of data is being collected.

- Policy 2 (Information Disclosure) - *"We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law."* In this policy, the SNS points out that users and their personal information are not products. Consequently, the SNS will not generate revenue from sharing users' information with third parties.

To summarize, as Table 3.2 shows, SNSs allow both the system and the users to specify privacy policies. In Facebook, the SNS provider has a system policy and every user also has a user policy. Similarly, some Diaspora PoDs have a system policy and every seed also has a user policy. In PrivacyWatch, the SNS provider can have a system policy depending on the privacy level (either "no privacy" or "soft privacy" levels), and every user also has a UPP. P2P SNSs such as SuperNova, PeerSoN and Safebook have no system policy, since there is not a central authority, but these SNSs have user policies set by peers. In the same manner, FOAF, set her own policies without the SNS provider. The existence of a system policy is defined by the SNS provider, and user policies may leads to the possibility of conflicts between all these privacy policies.

Table 3.2 – Administrative policy features in SNSs

	Facebook	*SuperNova*	*Diaspora*	*PrivacyWatch*	*PeerSoN*	*Safebook*	*FOAF*
	?+0	?+0	?+0	?+0	?+0	?+0	?+0
Administrative Policy Features							
System Policy	+	0	+	+	0	0	0
User Policy	+	+	+	+	+	+	+
System Conflict	+	0	0	0	0	0	0
User Conflict	+	0	0	+	0	0	0

3.2.5 Policy Conflicts

In SNSs, the diversity of privacy policies between users may represent conflicting preferences over a shared resource. Suppose three users (Alice, Bob and Charlie) interacting within the same SNS. Consider also a symmetric relation such that Alice is a friend of Bob, and Bob is a friend of Charlie. Alice uploads a document (e.g., a photo) on her webspace and tags Charlie in it. Suppose, on the one hand, that Alice authorizes only her friends to see the picture and, on the other hand, that Charlie has specified in his policy an interdiction, that nobody should be able to see the photos in which he appears. Bob wants to see a photograph shared by Alice and picturing Charlie, however Bob's access can be constrained by the policies of

Charlie. Most SNSs gives the highest priority to the user who publishes the resource. If such an "SNS strategy" is applied, the situation is somewhat unbalanced: Alice always gets what she wants, while Charlie never gets it. Note that Alice and Charlie cannot control the protection of the shared information without the assistance of the SNS policy management system. In fact, the SNS elects the data publisher policy for enforcement to solve conflict of preferences among policies specified by users.

Table 3.2 also summarizes the analysis of existing centralized and decentralized SNSs regarding both the resolution of conflicts between users policies (called user conflicts), and between system policy and user policy (called system conflicts). *System conflict resolution* in Facebook consists in a naïve approach in which the system policy always takes precedence on users' policies. *User conflict resolution* in Facebook is also simple since the publisher's decision has the highest priority. The same principle also applies to the existence of a *user conflict resolution* in PrivacyWatch, which includes the acceptance or rejection of a user UPP between the owner and the receiver.

As illustrated in Table 3.2, conflict resolution is still an open issue in both centralized and decentralized SNSs. In other words, privacy enforcement mechanisms that have been provided by existing SNSs are not satisfactory because they produce unbalanced control of the shared information: a conflict strategy resolution may benefit some users in detriments of other, leading to unfair situations. In this thesis, the system conflict is treated at the same level than user conflict since both can lead to unfair situations at enforcement time. Then, in order to handle conflicts between privacy policies, SNS provider and users need to achieve a mutual agreement to maintain privacy with fairness. The fairness of conflict resolution remains largely unresolved in the field of privacy management in centralized and decentralized SNSs. Chapter 5 describes the second contribution of this thesis: a novel conflict resolution mechanism based on an algorithm design to maintain equity.

3.2.6 Policy Management Architecture

To evaluate and enforce policies, an architecture for policy management is defined by the Internet Engineering Task Force (IETF) [MESW01, YPG00] and the ISO [ISO96], as shown in Figure 3.1. This architecture introduces three key components: PR (Policy Repository), PDP (Policy Decision Point), and PEP (Policy Enforcement Point).

When an access request is submitted, it is evaluated against the applicable privacy rules in a policy management architecture. In such an architecture, policy makers deposit policies in a PR. A PEP intercepts all access requests and forwards them to the PDP, which retrieves applicable policies from the PR. The PDP evaluates the policies and renders a response to the PEP. Finally, the PEP can either permit or deny access to the resource, according to the received request.

Actually each of these components is not necessarily unique, and its location could be centralized or decentralized. On the one hand, in centralized SNSs the central authority enforces the system policy and the users policies. On the other hand, from the perspective of decentralized SNSs, two main types of enforcement are possible [PFS14]: based on peers, or based on an external server (where data are stored). In the former, every user may have a personal server to enforce access control policies [Nas10], whereas the latter evolves

the introduction of an independent PEP, in the form of a external server or application to deal with many different PDPs. Moreover, subjects, resources, and actions may be different according to SNSs or application contexts.

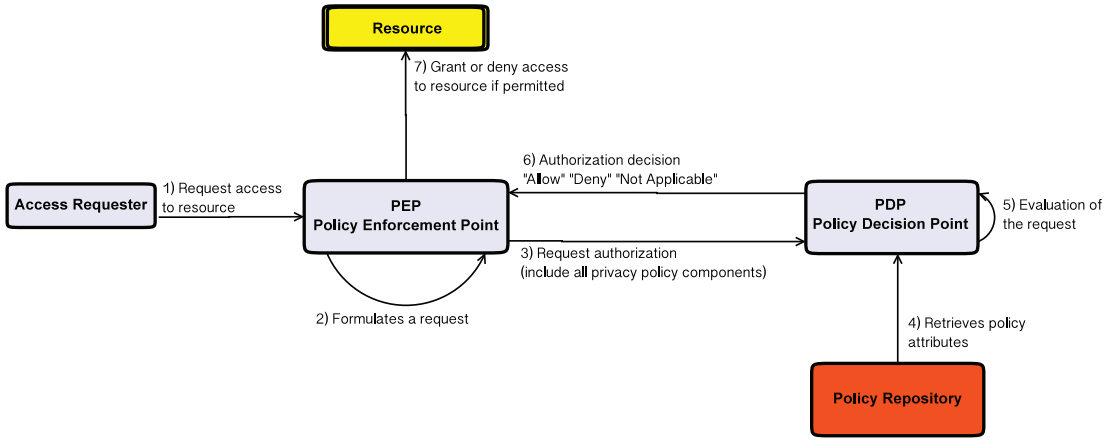

Figure 3.1 – Policy management architecture

3.3 Privacy Regulations for SNSs

Technological solutions and privacy policy management systems need to adhere to the conditions defined by regulations and laws to ensure users' rights.

Currently, there are no specific and adequate regulations to deal with the specific problem of data collection and processing in SNSs. The E.U. Data Protection Directive 95/46/EC (section 1.3.3) was conceived long before the advent of SNSs, and the new version is under revision. In fact, the new version of the Directive includes two legislative proposals to protect users' privacy in SNSs. The first is the *General Data Protection Regulation* [CP12], which regulates the free-flow of data and the protection of individuals, and the second is the *Police and Criminal Justice Data Protection Directive* [PtC13b], which regulates the activity of those who work in law enforcement for the purposes of prevention, investigation, detection or prosecution of criminal offences[8]. The core of the second proposal is to regulate and supervise law enforcement authorities, in order to avoid abuses when these authorities access and use SNS's data.

The definition provided by the Directive for data controllers is a "*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*" [PtC95]. Controllers must have appropriate technical and organizational measures to prevent unauthorized processing, taking into account the risks represented by the processing and the nature of the data.

The Directive only applies to data controllers that either process personal data in the context of the activities of an establishment within the European Union, or makes use of

[8] http://www.zdnet.com/blog/london/european-data-protection-law-proposals-revealed/1365

equipment situated in the E.U. (article 4.1 of the Directive). As a result, SNS providers that are established outside the E.U. such as Facebook, MySpace and LinkedIn, would not be subject to the Directive. However, the Article 29 Working Party [PtC02] is of the opinion that websites that place cookies on computer of E.U. citizens should be subject to the Directive, because they make use of equipments situated within the E.U. [ET10].

The Article 29 Working Party [PtC09] treats SNS service providers as data controllers under the data protection Directive, which imposes additional obligations when processing user data and privacy-friendly default settings. The Article 29 Working Party assumes that all data processing operations takes place on the data controller. Centralized SNSs rely on a centralized entity that essentially dictates the rules for all users, which is easy to control and to regulate. Conversely, without a central authority, decentralized SNSs require more expertise and efforts. Therefore, a significant level of legal uncertainty remains regarding which entity acts as data controller in decentralized SNSs.

3.4 Conclusion

This chapter focused on the protection of user privacy in SNSs. SNSs have proven to be a popular and useful entertainment platform, but they come with a cost in terms of privacy since users must provide personal information in order to use the system. Since information collection by a centralized entity is almost invisible, users' perception about the use of their personal information is obfuscated.

Over several researches that have been published or are ongoing, two types of approaches are adopted in this thesis to protect privacy rights: *decentralization of personal data*, and *policy conflict resolution*.

Decentralized SNS architectures have shown better results dealing with threats by keeping users' data in distributed space, where censorship and privacy issues that involve the SNS provider can be avoided. Since the proposed decentralized SNSs have significant differences in terms of services and architecture, a comparison based on a set of privacy criteria is necessary to establish their intrinsic characteristics. Chapter 4 proposes an analysis grid for privacy-related properties of SNSs.

Policy conflict resolution is an essential aspect to deal with privacy of shared data associated with multiple users. The solution considering that a privacy policy (either the system's or the data publisher's policy) always takes precedence on others policies leads to unfair situations. Chapter 5 proposes an analysis of the phenomenon and a novel conflict resolution approach that preserves the equity between users.

Part II

Enhancing Privacy Protection in SNSs

Chapter 4

An Analysis Grid for Privacy-related Properties of Social Network Systems

Privacy has proven to be difficult to achieve in commonly used SNSs, mainly because of their centralized infrastructure. Many alternative SNSs use decentralization of data and services in order to enhance privacy by keeping personal data with the users, on their personal devices, and by using PbD principles. In fact, decentralization seems a promising and efficient way to give users the control and ensure the privacy of their information. Decentralization tends to be seen as a transfer of control and services from service providers to users, which gives privacy protection a leading role in the specifications.

In decentralized SNSs, the absence of a central authority introduces certain difficulties in managing the infrastructure support. In particular, one should provide a balance between privacy protection on the one hand, and security, data availability and usability on the other hand. In fact, each SNS solution focuses on decentralizing some specific design points according to particular tradeoffs, based on the designer's preferences and architectural choices. However, designing a decentralized SNS allied to high abstract goals (e.g., embed "more privacy" in the design of the SNS) is a hard work. Designers in charge of building SNSs must cope with the difficulty to understand concepts in privacy regulations, as well as to consider user expectations, to use PETs to address users' privacy concerns, and to generate clear requirements to implement a functional system. Hasson et al. [HHA+14] stated that many designers perceive privacy as a theoretical-abstract concept rather than an applicable principle in designing information systems, such as SNSs. For Lederer et al. [LHDL04], one possible reason for the difficulty in designing privacy-enhanced systems is due to the variety of interpretations of the privacy concepts according to the designer's expertise. Therefore, the main challenges are related to the evaluation, comparison and classification of the existing

SNSs according to their core design choices, which are not obvious for designers.

In the rest of this thesis, the hypothesis that decentralization of data and services enhances the general level of privacy is assumed. It would therefore be useful to evaluate a given solution according to the design choices, in terms of decentralization. The first contribution of this thesis, described in this chapter, is the proposal of privacy-related properties in a multi-criteria analysis grid based on degrees of decentralization for design choices. Such a tool should be useful in a general PbD methodology for the development of SNSs. Indeed, based on such a multi-criteria analysis grid, it would be possible to organize privacy-related design choices in a rational fashion, in order to compare and classify SNSs based on sets of technical options. The first contribution of this thesis was published at *The* 3^{rd} *Atelier sur la Protection de la Vie Privée (APVP 2012)* [PMMPB12] and *The* 5^{th} *ASE/IEEE International Conference on Social Computing (SocialCom 2013)* [MPB13].

This chapter is organized as follows. Section 4.1 compares the approach proposed in this chapter with related works. Section 4.2 describes the degrees of decentralization. Section 4.3 describes privacy-related properties relevant to SNS design. Section 4.4 presents the multi-criteria grid analysis based on degrees of decentralization and its application to SNSs. In section 4.5, a lattice structure which can be used to systematically organize sets of privacy-related design choices into hierarchical structures is presented. Section 4.6 presents recommendations for the developers of SNSs. Section 4.7 presents the limitations of the contribution. Finally, some conclusion of this work are presented in section 4.8.

4.1 Similar Research Works

Aïmeur et al. [AGH10] have proposed a taxonomy of SNSs mainly according to the *data sovereignty principle*, understood as giving each user control over her personal data. Thus, the taxonomy focuses on privacy requirements such as the capacity for each user to define her privacy policy in a user-friendly way, tracking how her personal information is used or to report spam or abuse. Since data sovereignty basically means taking control from the central authority and giving it to the peers, it is a process of feature decentralization, captured by the classification in this thesis. Nonetheless, further properties of SNS can be used to improve the overall design without compromising user's privacy.

Paul et al. [PBS11] have also proposed a taxonomy of SNSs based on the degree of decentralization of basic SNS features, such as the architectural services or those related to data storage. Indeed, they identify SNSs such as FOAF and Diaspora, that use trusted servers to provide these features, and those that are based on P2P systems, such as Safebook and PeerSoN. However, they do not take into account the security aspects of privacy nor privacy policy management.

Thus, the aforementioned works do not cover the complete set of properties present for evaluating the level of privacy in SNSs. The taxonomy proposed in this chapter is based on the degree of decentralization of all the privacy-related properties, in relation to architectural services, storage, security and policy management.

4.2 Degrees of Decentralization

According to Baran [Bar64] and as depicted in Figure 4.1, there are three types of communication networks: centralized (a), decentralized (b) and fully decentralized (c)[1]. In a centralized network (star topology), all nodes are directly connected to a single centralized node, which is in charge of routing all communications, receiving data from sources and sending them to destinations. A decentralized network consists in several small centralized networks joined together, where each peripheral node is still dependent upon the proper functioning of its central node to route it. A distributed network does not have any centralized nodes: each node is connected to several of its neighbour nodes in a sort of grid arrangement with several possible routes to send data. In that case, if one route or a neighbour node disappeared, another path would be available.

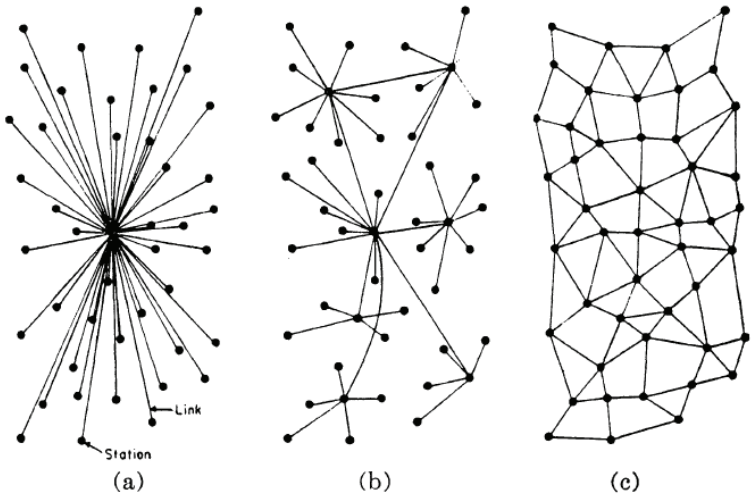

Figure 4.1 – Types of communication networks [Bar64]

Inspired by Baran's types of communication networks, in this thesis three degrees of decentralization are considered for SNSs: *(i) Centralized (C), (ii) Decentralized (D) and (iii) Fully Decentralized (FD).*

Centralized SNSs have a strongly hierarchical structure. There is a single and central authority with exclusive administration control. Centralized SNSs have a star network topology, meaning that all peers are directly connected to the central authority. Typically implemented as a client-server organization, the central authority is in charge of communication routing, friend search and content retrieval on behalf of the peers. The implication of such centralized services and infrastructures is that the central and unique authority has full control and holds all personal data of users. Even thought centralized SNSs make use of many physical servers, centralization in the context of this thesis is seen as the concentration of control in the unique authority.

A first step in decentralizing SNSs is to avoid the unicity of this central authority and to

[1]Baran's actually calls them "distributed".

allow for local, autonomous authorities to emerge. Such an organization corresponds to the **Decentralized** degree of decentralization. These systems have a hybrid network topology including a set of autonomous authorities with local administration control (sometimes known as "super-peers"), as well as ordinary peers. Therefore, decentralized SNSs in the context of this thesis is defined in terms of the distribution of control over multiple administrative authorities.

The next step towards decentralization is to build **Fully Decentralized** SNSs, where each peer can be seen as a punctual authority. Neither peers nor the network itself are organized in a hierarchical structure. All peers are equal in terms of provided services and control over data. Interactions are usually implemented through direct communication between peers. Therefore, fully decentralized SNSs in the context of this thesis is defined in terms of the distribution of control over the set of all users.

4.3 Privacy-related Properties for SNSs

In this thesis, the following assertion is assumed: SNSs built with more decentralization of data and services are likely to improve the general level of privacy, by avoiding the too significant influence of a central authority. While the majority of SNSs have two main functionalities (architectural services and storage, as described in section 2.2.3 Figure 2.2), decentralized SNS solutions (see section 2.4) focus on some specific design elements to decentralize data and services. These decentralized SNSs embed privacy features into their design to ensure minimum collection and disclosure of users' information. Some tradeoffs examples related to privacy features in the existing SNS approaches are presented as follows: Safebook increases security but decreases the usability of the system. SuperNova focuses on data availability but decreases security. PrivacyWatch balances usability benefits against the gradation of privacy levels (as introducing more restrictive levels of privacy may make the SNS more difficult to use). FOAF focuses on interoperability benefits against the loss of security. Some designs, such as PeerSoN and Diaspora, are focused on decentralizing the infrastructure of the SNS.

Since bringing more decentralization to the different aspects of SNS design improves the degree of privacy, it is interesting to evaluate each privacy-related property with respect to the degrees of decentralization in the SNS design. For this, the main design choices to be considered into the design of an SNS have been organized in four groups: architectural services, storage, privacy policy management and security aspects of privacy. Figure 4.2, which is an extension of Figure 2.2, presents this organization.

Each of these properties will be considered in parallel with a gradation along the decentralization scale previously introduced in section 4.2. All features, services and properties are considered with respect to all peers, and not simply to any peer, in order to take into account the actual impact of centralization or decentralization design choices.

4.3.1 Architectural Services

Architectural services cover the main services provided by the SNS, such as search, retrieval and communication. Note that these services, is formally defined in section 2.2.3, are detailed in the following. *Search* is the mechanism used to locate data and peers in SNSs. For the sake

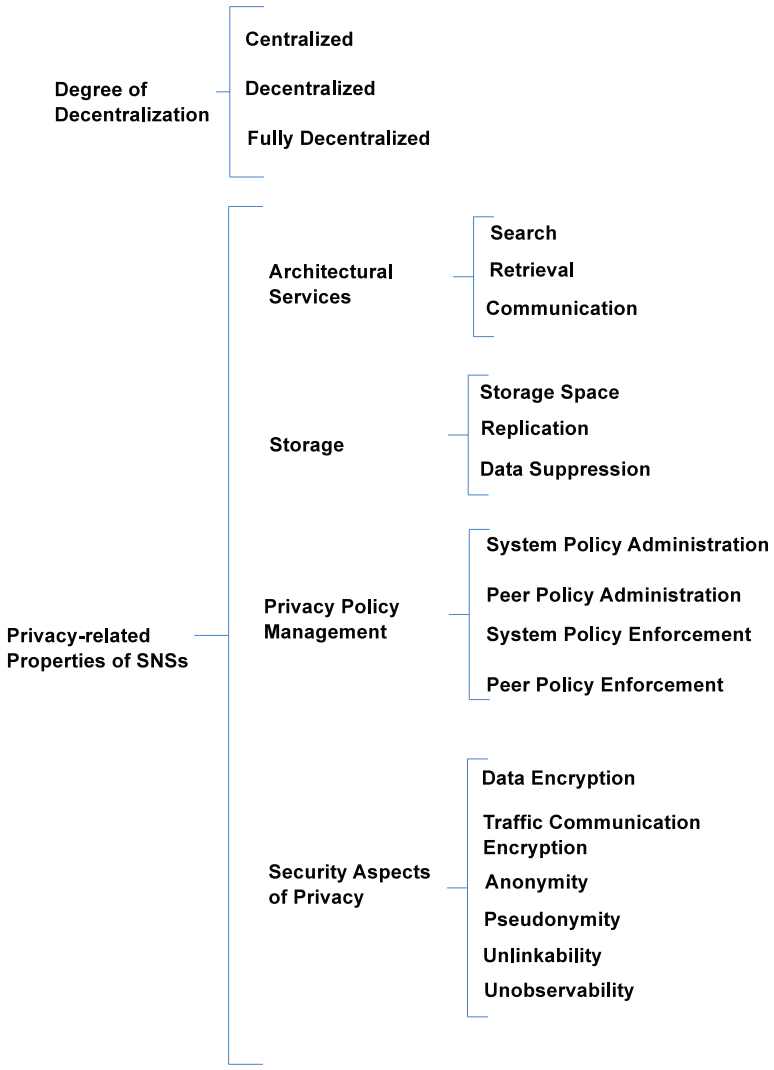

Figure 4.2 – Privacy-related properties for SNSs

of explicitness, a systematic definition of each property is adopted according to the different levels of decentralization are defined as follows for the "search" property:

- **Search**
  - *Centralized (C)*: only the central authority is in charge of searching friends/content for all peers;
  - *Decentralized (D)*: a given set of autonomous authorities are in charge of searching friends/content for all peers;
  - *Fully Decentralized (FD)*: the set of all peers are in charge of searching friends/content for all peers.

Retrieval is the mechanism through which data are exchanged among entities (i.e., peers, service provider and third-parties). Kirsch et al. [KGC06] pointed out that a social retrieval system is characterized by the presence of documents, queries, and users (i.e., users appear in their role as information producers or information consumers, queries relate to a user's informational needs, or describe a topic about which an individual possesses knowledge). The different levels of decentralization are defined as follows for the "retrieval" property:

- **Retrieval**
  - C: only the central authority is in charge of retrieving content for all peers;
  - D: a given set of autonomous authorities are in charge of retrieving content for all peers;
  - FD: the set of all peers are in charge of retrieving content for all peers.

Communication determines how data are transmitted among entities. The different levels of decentralization are defined as follows for the "communication" property:

- **Communication**
  - C: only the central authority is in charge of routing communications for all peers;
  - D: a given set of autonomous authorities are in charge of routing communications for all peers;
  - FD: the set of all peers are in charge of routing communications for all peers.

4.3.2 Storage

Storage describes how information is kept in the system. In this thesis, three properties are considered: storage space, replication and data suppression. Again these properties are already defined in section 2.2.3, but are detailed in the following. *Storage space* specifies where peer data are stored. There are several places where one can store user content, such as in the centralized SNS database or on a user's personal devices.

- **Storage Space**
  - C: only the central authority provides storage space for the data of all peers;
  - D: a given set of autonomous authorities provides storage space for the data of all peers;
  - FD: the set of all peers provides storage space for the data of all peers.

One important feature related to storage is data availability. To provide a high degree of availability in case of failure, SNSs often apply replication techniques to make data redundant. *Replication* indicates which entity is in charge of replicating profiles and resources, making data redundant in other machines. The type of replication can vary depending on the SNS implementation and each particular user's privacy policy. While, in some SNSs the complete profile can be replicated on friends' machines, in others only public data are replicated.

- **Replication**
  - C: only the central authority decides of the replication mechanism of all data replication;
  - D: a given set of autonomous authorities decide of the replication mechanism of all data replication;
  - FD: the set of all peers decide of the replication mechanism of all data replication.

Data suppression specifies which entity has the power to delete data from the system, including replicas (e.g., when a user closes her own account or requests an individual deletion). The General Data Protection Regulation described in section 3.3 is likely to provide a right to the deletion of personal data, where a user is able to withdraw her consent given to the SNS to use personal data, and third-parties should be notified about these requests [CP12]. The different levels of decentralization are defined as follows for the "data suppression" property:

- **Data Suppression**
  - C: only the central authority is able to delete data of all peers;
  - D: a given set of autonomous authorities is able to delete data of all peers;
  - FD: the set of all peers is able to delete data of all peers.

4.3.3 Privacy Policy Management

To characterize the security-related properties, it is first necessary to introduce an *attacker model* which allows to define three degrees of decentralization in the context of security and privacy. In this attacker model, the attacker is able to fully compromise one or several entities in the system, and her aim is to affect all the peers of the SNS with respect to a given property. This attacker model is taken into consideration to evaluate the architectural design strength. On the one hand, if an attacker goal is to solely affect a single peer or just a few, the task of the attacker is the same for a centralized architecture (the attacker affects a particular peer or the central authority), a decentralized architecture (the attacker affects a particular peer or the autonomous authority) or a fully decentralized architecture (the attacker affects a particular peer). On the other hand, if an attacker goal is to affect all peers, the task of the attacker is different for a centralized architecture (the attacker affects the total number of peers or the central authority), a decentralized architecture (the attacker affects the total number of peers or the given set of autonomous authorities) or a fully decentralized architecture (the attacker affects the total number of peers). Therefore, only the latter model allows to discriminate design choices based on the minimal number of entities that the attacker needs to compromise in order to reach her goal, as illustrated in Table 4.1.

This attacker can be qualified as "centralized", "decentralized" and "fully decentralized".

- **Attacker model**
  - C: the attacker can only compromise one central authority;

Table 4.1 – Minimal number of entities to be compromised depending on the attacker model

	The attacker wants to affect:	
Architecture	**1 peer**	**All peers**
Centralized	1	1
Decentralized	1	n
Fully Decentralized	1	*

n: given set of the autonomous authorities
*: the total number of peers

- *D*: the attacker can compromise a given set of autonomous authorities;
- *FD*: the attacker can compromise all peers.

Hence, the FD attacker is the most powerful one, and it should be more difficult to evade her than the others. These three type of attacker allow to grade the link between privacy policy management properties, security aspects of privacy properties and architectural choices.

Privacy Policy Management encompasses two types of privacy policies properties: policy administration and policy enforcement. The *policy administration* property describes which entity has the ability to define and modify policies, whereas the *policy enforcement* property specifies at which level the privacy policy is enforced. Both policy administration and policy enforcement may refers two different kinds of policies, namely system policies and peer policies. The *system policy* applies to the whole platform and governs the rights of the SNS provider, when it exists. *Peer policies* regulate privacy preferences among peers. The latter can be more or less rich and expressive depending on the systems: peer policies can range from imposed, system-wide rules to individually negotiated agreements between pairs of peers. The different levels of distribution are defined as follows for the "policy administration" and "policy enforcement" properties:

- **Policy administration - system policy**
  - *C*: only the central authority must be compromised in order to modify the system policy specification for all peers;
  - *D*: a given set of autonomous authorities must be compromised in order to modify the system policy specification for all peers;
  - *FD*: the set of all peers must be compromised in order to modify the system policy specification for all peers.
- **Policy administration - peer policy**
  - *C*: only the central authority must be compromised in order to modify peer policies specification for all peers;

  - *D*: a given set of autonomous authorities must be compromised in order to modify peer policies specification for all peers;
  - *FD*: the set of all peers must be compromised in order to modify peer policies specification for all peers.

- **Policy enforcement - system policy**
  - *C*: only the central authority must be compromised in order to modify the enforcement of system policy for all peers;
  - *D*: a given set of autonomous authorities must be compromised in order to modify the enforcement of system policy for all peers;
  - *FD*: the set of all peers must be compromised in order to modify the enforcement of system policy for all peers.

- **Policy enforcement - peer policy**
  - *C*: only the central authority must be compromised in order to modify the enforcement of peer policies for all peers;
  - *D*: a given set of autonomous authorities must be compromised in order to modify the enforcement of peer policies for all peers;
  - *FD*: the set of all peers must be compromised in order to modify the enforcement of peer policies for all peers.

4.3.4 Security Aspects of Privacy

Security Aspects of Privacy correspond to the mechanisms used to protect data confidentiality and integrity as well as peers' identities and activities. Most privacy regulations require that personal information should be securely kept, such as described by the E.U. Directive 95/46/EC.

Typically, security techniques such as encryption are used to protect the privacy of private information, whether it is transmitted as messages, or stored. In this thesis, two properties are proposed in direct relation with encryption: data encryption and traffic communication encryption.

Data encryption indicates which entity controls encryption and decryption of data.

- **Data encryption**
  - *C*: only the central authority must be compromised in order to decrypt data of all peers;
  - *D*: a given set of autonomous authorities must be compromised in order to decrypt data of all peers;
  - *FD*: the set of all peers must be compromised in order to decrypt data of all peers.

Traffic communication encryption indicates which entity controls encryption and decryption of communications.

- **Traffic communication encryption**
  - C: only the central authority must be compromised in order to decrypt the traffic from all peers;
  - D: a given set of autonomous authorities must be compromised in order to decrypt the traffic from all peers;
  - FD: the set of all peers must be compromised in order to decrypt the traffic from all peers.

The following four properties (anonymity, pseudonymity, unlinkability, and unobservability) are more specifically related to privacy protection, due to the fact that they characterize the exposure of personal information. The definition of these properties for protecting user's identities and activities is given by the Common Criteria security norm [ISO08]. In this thesis, these four properties have been adapted to the context of SNS. One should note that these four proposed properties are provided with respect to either as a central authority for (C), or as a set of autonomous authorities for (D), or anyone for (FD). Therefore, anonymity, pseudonymity, unlinkability, and unobservability are defined in a relative fashion in both C and D, while only FD is able to provide for these four properties absolute fashion.

Anonymity measures the capacity of a peer to perform an action within the SNS without disclosing its identity.

- **Anonymity**
  - C: anonymity is provided to users with respect to anyone but the central authority. Only the central authority must be compromised in order to de-anonymize all peers;
  - D: anonymity is provided to users with respect to anyone but one or several entities among a given set of autonomous authorities. This set of autonomous authorities must be compromised in order to de-anonymize all peers;
  - FD: anonymity is provided to users with respect to anyone. The set of all peers must be compromised in order to de-anonymize all peers.

Pseudonymity measures the capacity of a peer to perform an action within the SNS without disclosing its identity, while still being accountable for that action. It is worth noting that in anonymity and pseudonymity properties, the peer is not directly identified within the SNS (indeed, in anonymity, it is not possible to track peer identification). Pseudonymity usually relies on a trusted entity able to determine the user's identity based on a provided alias, and under certain legal circumstances.

- **Pseudonymity**

  - *C*: peer identity is masked to anyone but the central authority. Only the central authority must be compromised in order to revoke the pseudonymity of all peers;
  - *D*: peer identity is masked to anyone but one or several entities among a given set of autonomous authorities. This given set of autonomous authorities must be compromised in order to revoke the pseudonymity of all peers;
  - *FD*: peer identity is masked to anyone. The set of all peers must be compromised in order to revoke the pseudonymity of all peers.

Unlinkability measures the impossibility to establish whether two different actions have been performed by the same peer.

- **Unlinkability**
  - *C*: peer activities are unlinkable to anyone but the central authority. Only the central authority must be compromised in order to relate the actions of all peers;
  - *D*: peer activities are unlinkable to anyone but one or several entities among a given set of autonomous authorities. This given set of autonomous authorities must be compromised in order to relate the actions of all peers;
  - *FD*: peer activities are unlinkable to anyone. The set of all peers must be compromised in order to relate the actions of all peers.

Unobservability means the capacity of a user to perform an action without others being aware of this action.

- **Unobservability**
  - *C*: peer activities are unobservable to anyone but the central authority. Only the central authority must be compromised in order to be aware of the actions of all peers;
  - *D*: peer activities are unobservable to anyone but one or several entities among a given set of autonomous authorities. This given set of autonomous authorities must be compromised in order to be aware of the actions of all peers;
  - *FD*: peer activities are unobservable to anyone. The set of all peers must be compromised in order to be aware of the actions of all peers.

4.4 The Multi-criteria Analysis Grid

The privacy-related properties previously described can be organized in a two-dimensional grid: each line corresponds to one property (belonging to one of the four groups detailed in section 4.3), and each column to a degree of decentralization (described in section 4.2). The degree of decentralization has been chosen as the evaluation criterion because of the hypothesis that the distribution of services and data has a significant impact on the global level of privacy of the system. When evaluating existing systems, the following scale is adopted:

- *Unknown (?)* means that there is no available information in the SNS specification;
- *Nonexistent (0)* means that the privacy-related property is explicitly not addressed or not implemented in the SNS;
- *Centralized (C), Decentralized (D), and Fully Decentralized (FD)* are defined according to the definitions previously given.

Seven SNSs have been evaluated, considering their "default" setting configurations with respect to this multi-criteria analysis grid, including Facebook, as an example of centralized SNS, and the six decentralized SNSs described in section 2.4. Moreover, to analyze anonymity, pseudonymity, unlinkability, and unobservability properties, data search or profile search activities are considered since these properties may vary according to the type of activity. The multi-criteria analysis grid result is presented in Table 4.2.

4.4.1 Facebook

Architectural Services provided by Facebook to users are mainly based on a centralized architecture where search, communication and information retrieval services are operated by a central entity, the service provider at Facebook, and only the result is provided to users on the client side. Note that even though Facebook services are clustered and distributed for the sake of performance and load balancing, they are all controlled by a single entity, which implies in a centralized categorization.

Storage is centralized in Facebook's cluster of around 180,000 web and database servers. Facebook replicates the complete user profiles across their data center. Data suppression does not seems to be completely implemented [AGR13], because Facebook apparently remains with users' data for an undetermined time [MAYLL+09], arguing safeguard against legal measures.

Privacy Policy Management in Facebook is centralized for administration and enforcement regarding the system privacy policy, imposed by the contractual terms of Facebook. Users also have the ability to set up what is called in this chapter a peer policy, also focused on access control. More specifically, users can categorize their contacts in groups sharing the same access rights. Furthermore, users can specify which posts and photos the audience may access based on the following presets: "public", "friends", "custom", "close friends", "family", "acquaintances" and "only me". However, the policy of each user is stored on Facebook's central servers, which therefore makes a peer policy administration centralized, since only the central authority needs to be compromised in order to modify peer policies. Regarding enforcement, Facebook is in charge of both the system policy and peer policies, since decision about the actual delivery of information take place on their servers.

Security Aspects of Privacy rely on traffic communication encryption using SSL/TLS in order to provide security to the communication between the users' browser and Facebook's servers. Regarding this property, if Facebook servers are compromised, then the attacker will be able to decrypt all further traffic[2]. Data encryption is assigned to nonexistent, because

[2]Of course, if one trusted Certification Authority (CA) outside the system is compromised, then it allows for man-in-the-middle attacks. This is true for all platforms relying on SSL/TLS and is left outside the scope of this analysis.

Table 4.2 – The multi-criteria analysis grid applied at SNSs proposals

	Facebook					SuperNova					Diaspora					PrivacyWatch					PeerSoN					Safebook					FOAF				
	?	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*	*?*	*0*	*C*	*D*	*FD*
Privacy-related Properties																																			
Architectural Services																																			
Retrieval			C						FD				D						FD					FD					FD						FD
Communication			C						FD				D						FD					FD					FD						FD
Search			C					D					D					C					D					FD						FD
Storage																																			
Storage Space			C						FD				D						FD					FD					FD				C		
Replication			C					D					D						FD					FD					FD	?					
Data Suppression		0					?						D						FD		?					?					?				
Privacy Policy Management																																			
System Policy Administration			C				0						D						FD		0					0					0				
Peer Policy Administration			C						FD				D						FD					FD					FD				C		
System Policy Enforcement			C				0						D						FD		0					0					0				
Peer Policy Enforcement			C						FD				D						FD					FD					FD				C		
Security Aspects of Privacy																																			
Data encryption		0							FD		0								FD					FD			C			?					
Traffic encryption			C			?							D			?					?							C					C		
Anonymity			C					D					D					D					D					C				0			
Pseudonymity			C					D					D					D					D					C				0			
Unlinkability			C					D					D				C						D					C					C		
Unobservability			C					D					D				C						D						FD				C		

Facebook itself does not provide users with options to encrypt their data. In subsection 4.3.4, the assumption of the existence of a trusted authority for centralized degree characterizes the relative notion of the anonymity property. Therefore, the anonymity property is assigned to centralized, since only Facebook can link any action to a user's personal account, itself based on a real-life identity (per the Facebook terms of service). Pseudonymity is also assigned to centralized, for the same reason. Regarding unlinkability and unobservability, it must be noted that some actions (like people search or profile consultation) are visible and linkable only by Facebook as the central authority, while others (like status updating or public messaging) are visible and linkable by other users and also by Facebook. Given the level of granularity chosen in the analysis, it is concluded that unlinkability and unobservability are of the centralized kind in Facebook.

4.4.2 Safebook

Architectural Services in Safebook are fully decentralized, using the "matryoshka" structure, in which users form a P2P overlay network and cooperate to provide SNS services. Thus, users can directly search, communicate and retrieve information, using the resources of their neighbours instead of a centralized service provider.

Storage is provided by the matryoshka overlay, in which users store their own profiles. The social links between direct friends are then used to increase profile availability. This leads to protected and public data replication across direct friends. In spite of that, data suppression is not mentioned in the public specifications of Safebook.

Privacy Policy Management is fully decentralized in Safebook, since no central authority or super-peer exist for this purpose. Since there is no proper service provider to which policies could apply in Safebook, the notion of a system policy is absent. Therefore, system policy administration and system policy enforcement are assigned to nonexistent in Safebook. Peers are in charge of setting their own policies, and enforcement is performed directly by the peers within the collaborative P2P network. When defining peer policies, all attributes in a profile can be set with particular privacy policies and data can be categorized as private, protected or public. In the first case, the data are not published; in the second, data is encrypted before publication; in the third, data is published without encryption. In conclusion, peer policy administration and peer policy enforcement are fully distributed in Safebook.

Security Aspects of Privacy rely on key certification for data and traffic communication encryption, on the (Trusted Identification System) TIS for anonymity and pseudonymity, on the matryoshka structure for unlinkability and unobservability of the actions of the peers. More specifically, each peer first computes two pairs of public/private keys. Then, the peer communicates with the TIS which receives the user's public keys. The TIS generates a node identifier, a pseudonym and two certificates: the first links the node identifier with one of the public keys, and the second links the pseudonym with the other public key. The node identifier is used to build the matryoshka overlay, while the pseudonym allows to identify the peer in Safebook. The public key associated to the pseudonym is used to ensure end-to-end data encryption, hop-by-hop traffic encryption being based on the other public key. The matryoshka structure allows to have a hop-by-hop anonymity of the communications using recursion to hide the source of requests, as well as unlinkability and unobservability

from others peers in the SNS. Safebook assumes that direct peers are trusted, in the sense that they don't pose a risk to users' personal information. Then, both the TIS and direct trusted peers in the first ring in the matryoshka are able to link the user's identifiers (a user has different identifiers in each layer: a user ID in the SNS layer, a node ID in the P2P layer, and an IP address in the internet layer). It must be noted that the relative notion of anonymity in subsection 4.3.4 assumes the existence of a trusted authority for its centralized degree (also known as TIS in Safebook). Then, due to the level of granularity chosen in the analysis, we conclude that anonymity has similar characteristics to pseudonymity at this level of decentralization. Regarding the degree of decentralization criterion described in section 4.2, the TIS is a central authority that is in charge of distributing both the identifiers, the pseudonyms and the certificates. In addition, considering some actions such as a user searching for other users' data in the SNS, a request is forwarded to her direct friends until it reaches friends of friends of the targeted user's matryoshka. Thus, data and traffic communication encryption, anonymity, pseudonymity and unlinkability properties are of the centralized kind in Safebook, since only the TIS needs to be compromised in order to compromise all peers. For instance, if the TIS is compromised, then the attacker can revoke and re-issue certificates allowing her to perform a man-in-the-middle attack in P2P communication and make sure that data encrypted in the future can be decrypted by her[3]. Unobservability is assigned to fully decentralized because only direct trusted peers can track users' communication when these peers relay messages, such as when a user looks up another user's data in the SNS. It is interesting to note that although Safebook is presented as a decentralized SNS, the key security aspects may suffer from some of the drawbacks specific to centralized SNSs.

4.4.3 SuperNova

Architectural Services provided by SuperNova rely on a decentralized architecture for searching. Decentralized super-peers maintain a directory of users as soon as a user creates her profile in the SNS, and help them to search other peers. After a user establishes friendship in the system, communication and data retrieval are made directly by peers, in a fully decentralized manner.

Storage in SuperNova is decentralized in super-peers and storekeepers. Storage space is mainly in peers for personal data. Replication techniques in SuperNova use super-peers to provide available space for new nodes that do not have enough friends, as soon as they are added in the SNS. Another mechanism to improve data availability is storekeepers. Storekeepers are peers that have accept to keep replicas, only for their friends. Peers are able to view a list of super-peers and services they are providing (such as storage for peer data). Then, peers can decide on which component their information will be replicated in a encrypted form. Data suppression is not mentioned in the SuperNova specification.

Privacy Policy Management is fully decentralized in SuperNova regarding peer policy administration and enforcement. Peers are in charge of setting their own policies, categorizing data as private, protected, and public. All cryptographic and key management operations are performed by peers. In such an architecture, super-peers or storekeepers are only trusted

[3]This kind of man-in-the-middle attack is kept in scope of the study, since the point of failure lies within the system itself.

for the storage of protected and public data, and their existence is not associated with policy administration or enforcement. Since the notion of a system policy (administration and enforcement) is absent, "nonexistent" is then assigned to the grid.

Security Aspects of Privacy addresses data encryption in a fully decentralized fashion (i.e., the peer is the entity in charge of data encryption). In SuperNova, a peer can search another peer profile by consulting the user list in the system maintained by super-peers. The user list contains every user's id and the respective public information. In subsection 4.3.4, the assumption of the existence of a trusted authority for decentralized degree characterizes the relative notion of anonymity property. Then, anonymity, pseudonymity, unlinkability and unobservability properties are assigned to decentralized, since super-peers are able to identify users in the SNS, as well as seeing and linking actions performed by peers.

4.4.4 Diaspora

Architectural Services in Diaspora are provided by PoDs (i.e., servers) in a decentralized form. These services include retrieval of profile details for seeds (i.e., clients), search for friends in other PoDs, and communication in the SNS.

Storage is decentralized in the PoDs. PoDs provide storage space, and users are able to decide on which PoD their information will be stored. PoDs replicate a user's data through other PoDs that share this user's connection. Data suppression is implemented as soon as a user deletes her account in the PoDs, which is propagated to other PoDs that follow her.

Privacy Policy Management is decentralized for administration and enforcement. Diaspora mentions theoretical privacy policies based on encryption, although these policies do not seem to be currently implemented. Each Diaspora PoD administrates its own system policy and every seed manages her own policy. However, this policy is stored on a decentralized PoD server. Therefore, peer policy administration is decentralized since only a given set of peers need to be compromised in order to modify all peer policies. Both system and peer policy enforcement are performed at PoD level.

Security Aspects of Privacy rely only on SSL/TLS to enable traffic communication encryption between the seeds' browser and PoDs, between PoDs, as well as when a seed communicates with another seed. Thus, traffic communication encryption is assigned to decentralized because each PoD manages and stores their own SSL keys. Data encryption is assigned to nonexistent, since data encryption is not implemented in practice. In subsection 4.3.4, the assumption of the existence of a trusted authority for decentralized degree characterizes the relative notion of anonymity property. Then, anonymity, pseudonymity, unlinkability and unobservability properties are assigned to decentralized, since PoDs can link any action (such as search profile) to a seed's personal account, and be able to see and link all actions performed by seeds.

4.4.5 PrivacyWatch

The default setting in PrivacyWatch, called the "full privacy" level, is considered. *Architectural Services* are handled by a centralized SNS provider in PrivacyWatch, regarding the search property. Each user installs her own web server to directly retrieve information among

peers and communication in a fully decentralized form.

Storage is performed in the Client Privacy Manager (CPM) component in the peer-side. The CPM contains two databases: the XML database in the key manager module, and a user database in the client access controller module. The XML database stores all keys of the user and her friends. Storage space is mainly in the user database, where data and UPP are kept. Replication strategies are centralized in two servers: the SNS and the Mail providers. The SNS provider stores only encrypted data, whereas the Mail provider stores encrypted keys and UPP. Thus, the replication property is of the fully decentralized kind in PrivacyWatch, since this property is under peer control even though data is replicated on centralized servers. Data suppression is also under peer control in the PrivacyWatch specification.

Privacy Policy Management depends on the privacy levels and groups classification defined in the application. In the privacy policy, each piece of data of the profile can be characterized as poisonous, harmful, harmless or healthy [AGH09]. As a result, Aïmeur et al. [AGH09] propose privacy levels associated to the amount of the information that should be encrypted. The default setting recommended for "no privacy" is to not encrypt data, "soft privacy" suggests to encrypt poisonous data, "hard privacy" suggests to encrypt poisonous and harmful data, and "full privacy" suggests to encrypt all data. The UPP links each piece of data to a predefined privacy level. Each level determines how much information the user wants to share with the provider. Regarding system policy enforcement, the SNS provider controls access to information in "no privacy" and "soft privacy". Regarding peer policy enforcement, users controls the enforcement of policies when privacy level is set up as "hard privacy" and "full privacy". In the "full privacy" level, the SNS server is only trusted with the storage of an encrypted version of the user's personal information. Therefore, when considering only "full privacy" is possible to conclude that all the properties in privacy policy management are fully decentralized, since the peer is in charge of policy administration and enforcement of all relevant policies.

Security Aspects of Privacy rely on encryption and group signature schemes. Data encryption is fully decentralized since each user generates the keys used for encryption and decryption. Traffic communication encryption is assigned to unknown because there are not details related to this property. PrivacyWatch relies on anonymous credentials by using a group signature scheme. These credentials allow an entity to reveal the group to which she belongs without having to disclose her identity to the SNS provider. Pseudonymity is assigned to decentralized because the group manager (i.e., a user of the SNS in charge of distributing private signature keys for each member of the group) can identify the user if necessary. It must be noted that the relative notion of anonymity in subsection 4.3.4 assumes the existence of a trusted authority for the decentralized degree (also known as group manager in PrivacyWatch). Due to the level of granularity chosen in the analysis, anonymity has similar characteristics to pseudonymity for this degree of decentralization. Therefore, both properties are of the decentralized kind since only the set of group managers need to be compromised in order to de-anonymize or revoke the signatures of all peers. Since the SNS provider is able to link and visualize the user's actions for some activities such as searches for friends profiles, unlinkability and unobservability are both centralized in PrivacyWatch.

4.4.6 PeerSoN

Architectural Services in PeerSoN have fully decentralized properties for retrieval and communication. These properties are based on direct content exchange among peers, and communication between peers are performed directly when they are online. Search for peers or files are decentralized since peers request information to the OpenDHT, consisting of super-peers to provide lookup metadata. A peer that decides to become a super-peer therefore has to maintain a list of peers IDs. Then, the OpenDHT sends to the peers the requested information.

Storage and data availability in PeerSoN occur in a fully decentralized fashion, since each user stores her own data, and the OpenDHT is used to store metadata. Data that are encrypted (protected) are replicated in random peers, but data suppression is not mentioned in PeerSoN.

Privacy Policy Management is fully decentralized in PeerSoN regarding peer policy administration and enforcement. Peers are in charge of setting their privacy policy and distributing encryption keys to authorized friends. In order to decrypt data, these keys are then shared and distributed with friends. It is important to note that super-peers provide lookup services, but not policy management. Then, system policy administration and enforcement are assigned to nonexistent in PeerSoN.

Security Aspects of Privacy address only data encryption to enhance privacy. In this context, a user can encrypt data and establish access control with appropriate key sharing and distribution through the existence of the public-key infrastructure. In PeerSoN, a peer can search another peer profile or content by asking super-peers for information. In subsection 4.3.4, the assumption of the existence of a trusted authority for decentralized degree characterizes the relative notion of anonymity property. Then, anonymity, pseudonymity, unlinkability and unobservability properties are assigned to decentralized, since super-peers are able to identify users in the SNS, as well as seeing and linking actions performed by peers.

4.4.7 FOAF

Architectural Services in FOAF are performed by users for retrieval, communication, and search by using the “foaf:knows” property. More specifically, communication is performed through using “foaf:knows” and “rdfs:seealso” properties to connect distinct FOAF files together.

Storage, in the FOAF framework, does not implement replication techniques and a user stores her FOAF profile (it can be used to describe a user on a detailed level) in a trusted centralized server. In the FOAF specification, data suppression is not mentioned.

Privacy Policy Management is centralized in FOAF regarding peer policy administration and enforcement. Users are in charge of specifying privacy policies to restrict access to their data. However, the policy of each user is stored on centralized servers, which therefore makes peer policy administration centralized, since only the central authority needs to be compromised in order to modify users policies. Peer policy enforcement is also assigned to centralized, for the same reason. Since the centralized server is only used to provide storage of the user’s personal information, policy administration and enforcement are assigned to

nonexistent in the grid.

Security Aspects of Privacy rely on WebID protocol, which provides a mechanism to authenticate and identify users to the server, using SSL certificates to enable traffic communication encryption. When a user searches another user, it is necessary to obtain the corresponding URI. This URI corresponds to a unique WebID that references the server in which the FOAF profile is stored. Then, anonymity and pseudonymity properties are assigned to nonexistence. Since the trusted server is able to link and visualize the user's actions for some activities, such as searches for friends' profiles, unlinkability and unobservability are both centralized.

4.5 Interpretation in a Lattice Structure

The result of the multi-criteria analysis grid can be used to analyze SNSs in regards to a set of design properties. Indeed, the evaluation of design properties is a common problem, although many alternatives in terms of criterion sets are currently available [AHA11]. In this thesis, lattices are proposed as an appropriate technique not only to evaluate, but also to classify and to visualize SNSs.

Lattices provide a mathematical foundation by systematically ordering pairs of objects into a hierarchical structure. According to Davey [DP90], an order is a binary relation on a set of objects in mathematical terms. A binary relation R on a set V is called an order relation if and only if it is reflexive, antisymmetric and transitive.

- Reflexivity: $\forall x \in V, xRx$;
- Antisymmetry: $\forall (x, y) \in V^2, xRy \; and \; yRx \Rightarrow x = y$;
- Transitivity: $\forall (x, y, z) \in V^3, xRy \wedge yRz \Rightarrow xRz$.

Additionally, if xRy or yRx for all x, y in V, then the order is total, otherwise it is partial. An ordered set (V, $\leq$) is a lattice if it is a partially ordered set in which any two elements x, y have a supremum $x \vee y$ (the so-called least upper bound), and an infimum $x \wedge y$ (the so-called greatest lower bound). Lattices are useful since they allow to represent a partially ordered set of objects in a diagrammatically fashion. In this thesis, the lattice diagram is built considering the degrees of decentralization as a total order relation. A relation between degrees of decentralization is expressed using the operator "<", defined as:

$$\text{nonexistent } (0) < \text{unknown } (?) < \text{centralized } (c) <$$

$$\text{decentralized } (d) < \text{fully decentralized } (fd)$$

SNSs near the top node are then considered "more decentralized" in general, and therefore better for privacy according to the hypothesis in this thesis considering the evaluation criterion described in section 4.4.

Classification based on this kind of lattice has been done considering *chains* and *levels*. A chain is a sequence of elements in which all pairs of elements are comparable [Pra14].

Two SNSs are in the same chain if they can be directly compared according to the lattice structure and its partial order. A relation between SNSs based on chains is expressed using the operators "$\lhd$", defined as: $a \lhd b$ is a transitive closure of the relation saying that a is lower than b in some chain. If two SNSs cannot be related that way, then they will be compared in levels. A level is a position on a stratum of the lattice. The SNSs are at the same level if they appear in the same stratum of the lattice (i.e., at the same distance from the top node). A relation between SNSs based on level is expressed using the operators "$\prec$", defined as: $a \prec b$ means that a is in a lower stratum than b. If two SNSs are at the same level but in different chains, it is not possible to compare them without making priority choices among the privacy-related properties.

A simplified example, limited to two properties, is presented in Figure 4.3. Note that lattice structures increase exponentially in size as the number of properties grows, therefore it is not easy to represent the full structure. This lattice illustrates the fact that the analysis grid results can be used as an input to compare SNSs. The lattice in Figure 4.3 is a projection on two privacy-related properties: data encryption, represented by the letter A, and traffic communication encryption, represented by B. Both A and B range over the set of values $\{FD, D, C, ?, 0\}$.

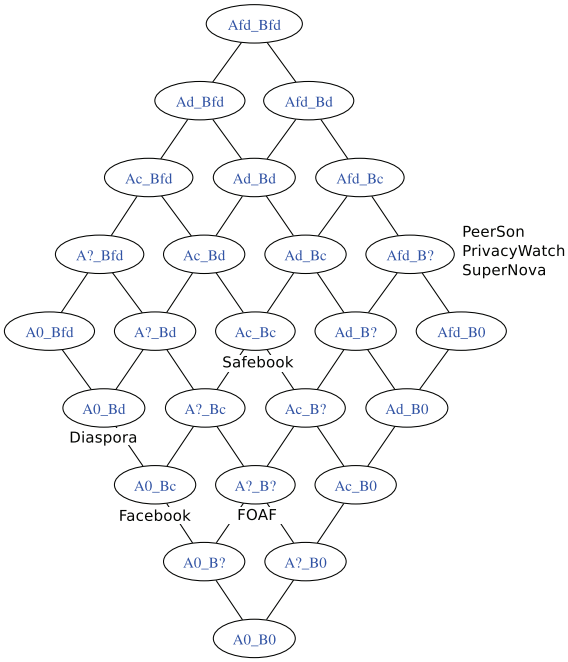

Figure 4.3 – Lattice based on the data encryption (A) and traffic communication encryption (B) properties

The lattice in Figure 4.3 allows to identify significant hierarchical relationship based on chain comparisons, represented by the following expressions:

$$FOAF \lhd PeerSoN, PrivacyWatch, SuperNova \tag{4.1}$$

$$Facebook \lhd Safebook \tag{4.2}$$

$$Facebook \lhd Diaspora \tag{4.3}$$

$$FOAF \lhd Safebook \tag{4.4}$$

Expression 4.1 means that PeerSoN, PrivacyWatch, SuperNova are better than FOAF with respects to the considered properties. The same kind of interpretation can be made for expressions 4.2, and 4.3. Expression 4.4 is obtained by transitivity.

The lattice in Figure 4.3 allows also to identify another significant hierarchical relationship based on level comparisons but in a less direct way, represented by the following expression:

$$Diaspora \prec Safebook \tag{4.5}$$

Expression 4.5 allows to conclude that Safebook (5^{th} level) is better with respect to the considered properties than Diaspora (4^{th}level), only if it is accepted that the importance of a one-level difference on one property is always the same, for all levels and for all the properties considered. Therefore, comparisons based on levels might be unreasonable in many cases.

4.6 Making Recommendations to Developers

Based on the multi-criteria analysis grid and the lattices from the previous sections, the following design recommendations have been derived in an attempt to help developers to build privacy-enhancing SNSs. During the conception of SNSs, recommendations can be important to improve designing in a reasonable manner, specially in order to comply with privacy regulations such as the European Regulation described in section 1.3.3. Despite the importance of these regulations, there is no general agreement about how much privacy should be built into SNSs [SC09]. As a consequence, some recommendations can be more or less appropriate, depending on the designer's preferences and goals.

From centralized to distributed SNSs, the design of services and data management often address tradeoffs, as identified in section 4.3. These tradeoffs, when related to privacy, have led SNS designers to focus on *quality* aspects such as *confidentiality, integrity, availability, performance, and usability*. It can be noted that in the information security literature, the triad of confidentiality, integrity, and availability are generally referred altogether as security attributes. In this thesis, the notion of information security is embedded in confidentiality and integrity quality aspects (resulting in the "confidentiality & integrity" quality) because both are related to personal data, while availability is a critical aspect for SNS infrastructures

[Nar12]. These quality aspects, which can impact the protection of the user's privacy, are defined as:

Confidentiality & Integrity: preserve unauthorized disclosure and modification of personal information.

Availability: provides access of data and services to users.

Performance: measures the efficiency of a SNS in terms of response time.

Usability: is a measure of how easy features and operations are for users.

These qualities, when considered in the context of decentralized SNSs, correspond to benefits and challenges that need to be identified and analyzed before their development. In order to provide better recommendations to designers, some combinations that could be deemed interesting for the development of privacy-enhanced SNSs will be examined in the section that follows.

4.6.1 Composition of Properties

Given the number of different privacy-related properties of SNSs governed by distinct degrees of decentralization, it seems necessary to reason about the compositional aspects of these properties. The composition of properties at a given of decentralization level should be analyzed to asses the synergy of the resulting composition. Although privacy-related properties are organised in four groups (architectural services, storage, privacy policy management and security aspects of privacy), the strength of certain compositions are produced by combinations ranging over different groups. Therefore, the designer should give attention not only to relationships between properties within the same group, but to distinct groups as well. By understanding the implications of the composition of properties, it is possible to provide recommendations about the design and development of SNS in a reasonable manner. In this thesis, eight compositions (C1 through C8) classified in four groups have been identified in Table 4.3 as bearing certain strengths and limitations, and are described as follows.

C1. ***Storage Space (C)* × *Replication (C)* × *Data Encryption (FD)*:** One of the most important design decisions for any SNS is to determine the data storage strategy. Looking from the traditional centralized SNSs perspective and their respective users, a first step to continue using these systems while protecting users' privacy is to integrate some sort of encryption technique. In this case, let us consider the combination of a centralized storage space and replication along with fully decentralized data encryption, represented by *Storage Space (C)* × *Replication (C)* × *Data Encryption (FD)* (further information in section 4.3). *Storage Space(C)*, along with the *Replication (C)* property from the "storage" group, results in a potential positive impact on performance. The *Storage Space (C)* of the data may rely on the segmentation of users' content across a number of servers to optimize performance

and deliver continuous services to users [Tra12]. Centralized SNSs such as Facebook and Twitter uses a DHT called "Cassandra" to ensure high availability. The Cassandra storage system duplicates data across multiple data centers using different replication policies, all of them controlled by a central authority. These *Replication (C)* schemes often lead to faster response times in replicas. However, the combination of *Storage Space(C)* × *Replication (C)* properties may result in a potential negative impact on availability because this centralized set of data servers can be subject to Distributed Denial-of-Service (DDoS) attacks [CMS10]. This kind of attack may interrupt the communication service for some or all users, making the SNS unavailable because the central authority has become a single point of failure. Solely, the combination of properties *Storage Space (C)* × *Replication (C)* only allows efficient and rational centralized storage of users' data, such as in Facebook in the analysis grid in section 4.4. If all data collected from all users are centrally stored without protection, or if encryption is controlled by the central authority, then there is no way to get data hidden from the SNS provider.

When adding the *Data Encryption (FD)* property, from the "security aspect of privacy" group, an improvement with potential positive impact on confidentiality & integrity can be achieved. Given the *Data Encryption (FD)* property, the stored information is then protected from the SNS provider, allowing each user to manage her own cryptographic keys. The use of *Data Encryption (FD)* also results in a potential negative impact on performance and usability: data encryption comprises key creation, key distribution, as well as file encryption and decryption, which introduce additional computational load for the exchange of information, incurring in a significant performance overhead [PFS14]. Moreover, the use of cryptography may bring difficulties for users in terms of usability such as the comprehension on how to set up public keys.

C2. ***Storage Space (D)*** × ***Replication (D)*** × ***Data Encryption (FD)*** **:** In decentralized SNSs, maintaining high availability for data published by users is a major issue because the original source of the content can be offline [PGW+08, SD12]. A gradual variation of the previous composition (*Storage Space (C)* × *Replication (C)* × *Data Encryption (FD)*) is to decentralize storage space and replication along with the fully decentralized data encryption property, which is represented here by *Storage Space (D)* × *Replication (D)* × *Data Encryption (FD)*. The major difference between centralized and decentralized compositions is that decentralized SNSs offer better data confidentiality because there is not a single central authority in control: thanks to the *Storage Space (D)* property there are autonomous authorities storing data for sets of users, but not for the whole SNS. Moreover, decentralized architectures use *Replication (D)* to replicate data on various servers, ensuring permanent availability of resources and providing enough storage capacity, resulting in a potential positive impact on availability, given that decentralized SNSs are more resilient to failure. Communication flows within autonomous authorities, even if parts of a system are disrupted, because the collaborative network usually remains partially available. The analysis grid shows that the choice of *Storage Space (D)* × *Replication (D)* has been made by the designers of Diaspora. Although decentralized storage allows users to set up their own servers, towards a better control, published content is still vulnerable to potential exposure to a very large number of autonomous authorities. To minimizes the risk of exposed content, the property *Data Encryption (FD)* should be used, although affecting performance

and usability.

C3. *Storage Space (FD) × Replication (FD) × Data Encryption (FD)*: Let us now consider the combination of fully decentralized storage space, replication, and data encryption properties, which are represented by *Storage Space (FD) × Replication (FD) × Data Encryption (FD). Storage Space (FD)* may result in two potential negative impacts: on performance, especially for mobiles who may not be able to handle the intense bandwidth needed for content delivery due to some constantly accessed data, and on usability, since the installation of a distributed SNS application may require a significant amount of storage space. *Replication (FD)* may induce a positive impact on availability, since peers control replication over several strategies to distribute replicas: friend peers, random peers, super-peers, and centralized servers providing redundancy of data stored. Recent studies have shown that, depending on the storage capacity and replication, high data availability can be achieved when content is stored with the most active friends [NPA12], even with a low number of replicas [TKF11]. However, *Replication (FD)* may also have a negative impact on performance due the to the high churn rate in P2P SNSs, leading to latencies in the propagation of uploads and thus to a slower time response. The analysis grid shows that the choice of *Storage Space (FD) × Replication (FD)* has been made by PrivacyWatch, PeerSoN, and Safebook.

Although *Storage Space (FD)* allows users to keep personal data on their own devices, published content is still vulnerable to exposure to a very large number of users. To minimize risk of users' content exposure, the *Data Encryption (FD)* property can be used, although affecting performance and usability. The *Storage Space (FD) × Replication (FD) × Data Encryption (FD)* combination is currently adopted in PrivacyWatch and PeerSoN.

Recommendation: C1 is indicated to improve confidentiality & integrity in Centralized SNSs, although decreasing in availability, performance, and usability, whereas C2 and C3 combine high availability with confidentiality & integrity when decentralizing personal information. While C2 and C3 compositions suffer with usability and performance issues, C3 presents a more significant impact on these qualities than C2.

C4. *Search (C) × Unobservability (C) × Unlinkability (C) × P.A. Peer Policy (C)*: Another strength of services in the SNSs context is information *Search*. Such a feature involves searching for friends (as well as being found by them), and content discovery. After receiving user's request, the centralized servers query the SNS's databases to find the friend or content that is sought. The *Search(C)* property from the "architectural services" group results in two potential positive impacts: on performance, enabling high search capabilities because of the existence of a centralized entity capable to find the index list of all users within the SNS, and on usability, since from the developer's perspective, a centralized design has the advantage of being simple to implement. However, *Search(C)* also results in a potential negative impact on confidentiality & integrity, since the centralized entity usually allows the observation and linkability of users' content access. Therefore, centralized search is highly correlated to centralized unobservability and unlinkability, which is represented by *Search (C) × Unobservability (C) × Unlinkability(C)*. The analysis grid shows that this choice of composition has been made in Facebook and PrivacyWatch. A mechanism that might be employed to compensate *Search(C)* would be Private Information Retrieval (section 1.5) which would allow users to search information without compromising their con-

fidentiality by hiding queries and results from the SNS provider, even though this solution is computationally intensive and incapable to protect the user identity. Moreover, *Unobservability (C)* × *Unlinkability(C)* allows visibility and linkability of some actions by other users in the SNS. In this regard, users are allowed to specify privacy policies restricting access over content, which is represented as *P.A. Peer Policy (C)*. Typically, the default privacy setting of a *P.A. Peer Policy (C)* sets the visibility and accessibility of personal information (e.g., basic profile data, pictures, gender, likes, etc) to the entire Internet. Since in practice only few users change the default settings, *P.A. Peer Policy (C)* may result in a potential positive impact on availability because more personal information is accessible to a large number of users, but it might have a negative impact on the user's privacy by potentially increasing privacy leaks.

C5. ***Search (FD)* × *Unobservability (FD)* × *Unlinkability (FD)* × *P.A. Peer Policy (FD)*:** Let us consider now a composition that assumes fully decentralized search, unobservability, unlinkability and peer policy administration, represented by *Search (FD)* × *Unobservability (FD)* × *Unlinkability(FD)* × *P.A. Peer Policy (FD)*. *Search (FD)* may result in a negative impact on performance. For instance, P2P SNSs based on unstructured topologies (e.g., SuperNova) may use flooding queries, generating a large volume of network messages and thus inducing a serious increase in response time. In contrast, structured topologies based on DHTs (e.g., Safebook uses Kademlia; PeerSoN uses OpenDHT) are more efficient since they are able to search data directly, but long communication chains also hamper performance. In fully decentralized SNSs, users' requests are routed among several nodes in the P2P substrate to find paths in a SNS. As a consequence, *Search(FD)* may result in a potential negative impact on confidentiality & integrity, since users may be able to link (i.e., *Unlinkability(FD)*) and detect the presence of a specific user (i.e., *Unobservability (FD)*) within the SNS, depending on how communications are encrypted. Once the sought content is reached, privacy policies regulate access to it, which is represented here by *P.A. Peer Policy (FD)*. *P.A. Peer Policy (FD)* allows flexibility at different levels of granularity to express more control over access decisions, which may result in a negative impact on availability, since less content is exposed, but might result in a positive impact on confidentiality & integrity, by providing data only to authorized users in the SNS. In addition, this composition results in a potential negative impact on usability, because it often requires more efforts from users during the installation and configuration of the SNS.

Recommendation: C4 is indicated to improve availability, performance, and usability, although decreasing confidentiality & integrity. Conversely, C5 expresses an improvement on confidentiality & integrity, but causes usability, performance and availability problems.

C6. Anonymity × Pseudonymity: Some privacy properties seem to have constraint in their combination. For instance, a potential incompatible combination is by assuming fully decentralized *Anonymity (FD)* and *Pseudonymity (FD)*. Both properties are related to each other because they aim to protect the real identity of a user in the SNS. Despite their relationship, anonymity and pseudonymity are distinct concepts. On the one hand, *Anonymity (FD)* is based on the idea that a user does not reveal her identity within the SNS. As a consequence, users interactions and activities are impossible to be associated with their identities. This property may foster people's freedom of expression and honesty, but lacks accountability [JM98]. On the other hand, *Pseudonymity (FD)* enables to relate the user's

actions with respect to a pseudonym for accountability purposes, but without disclosing her identity. By definition, these properties have different goals and it may not be possible for a SNS to simultaneously provide both *Anonymity (FD)* and *Pseudonymity (FD)* properties. In the analysis grid, it is possible to find a balance between these incompatible design properties due to the level of decentralization. For this reason, similar characteristics are assigned to *Anonymity (D)* × *Pseudonymity (D)*, and *Anonymity (C)* × *Pseudonymity (C)*.

Recommendation: Users should have the option to avoid identifying themselves with real identities. Anonymous usage options should be given to users. The pseudonymity property can be considered as a useful alternative to take advantage of several personalized services. In this case, pseudonym identities are chosen for the SNS design and should be changeable.

C7. *P.E. Peer Policy (C)* × *Storage Space (C)* × *Retrieval (C)*: Another major factor that contributes to ensure users' data control is usually through the management of policies. Let us consider a SNS with centralized peer policy enforcement, storage space and retrieval properties, represented by *P.E. Peer Policy (C)* × *Storage Space (C)* × *Retrieval (C)*. *P.E. Peer Policy (C)* may result in a potential positive impact on performance because peers' policies and data are maintained by only one single authority. This central authority provides *Storage Space (C)* for the policies of each user, evaluating and enforcing each access decision. Afterwards, the central authority performs *Retrieval (C)* of data, recovering the corresponding record for enforcement. This centralized design combination can also result in a potential positive impact on usability since it has the advantage of being a simple service implementation. The advantages of centralization come with drawbacks regarding the negative impact on confidentiality & integrity, since the central authority controls the information and policies of all users, and on availability because the central authority can become a single point of failure and thus become unavailable in case of a DDoS attack.

C8. *P.E. Peer Policy (FD)* × *Storage Space (FD)* × *Retrieval (FD)*: Let us consider now a fully decentralized peer policy enforcement, storage space and retrieval properties, represented by *P.E. Peer Policy (FD)* × *Storage Space (FD)* × *Retrieval (FD)*. Solely, considering *Storage Space (FD)* in a first glance may result in a positive impact on confidentiality & integrity, because each user is able to store her own data and policy. However, *Storage Space (FD)* without replication property may result in a negative impact on availability when the user is offline, causing problems to access the data source. When combining *Storage Space (FD)* × *P.E. Peer Policy (FD)*, the composition may now express a negative impact on performance due to the fact that the enforcement of privacy policies occur with the help of some encryption technique, which brings difficulties regarding key distribution and computational load. After the enforcement of privacy policies, users then are able to perform *Retrieval (FD)* of data in order to recover their corresponding data records. While this fully decentralized design combination can have a negative impact on usability since decentralized management of users' policies increase accountability, time consumption and demands basic knowledge of cryptography, it also express a positive impact on confidentiality & integrity by protecting user's content through encryption.

Based on *P.E. Peer Policy (FD)*, every user has a Policy Decision Point - PDP (section 3.2.6) that handles policies. Conversely, in *P.E. Peer Policy (C)* the centralized management contains PDP and Policy Enforcement Point - PEP, facilitating how the central authority

dictates which user has access to which resource, as well as easing the application of conflict resolution strategies for all users, as previously presented in section 3.2.5. It is important noting that the majority of centralized SNSs are able to solve policy conflicts and enforce access decisions for all their users, given priority to the ones who publish shared resources. However, this kind of simplistic conflict resolution might generate unfair situations, since some users can have their policies more enforced than others. Due to the complexity of privacy policy conflict management, in chapter 5 is presented a novel conflict resolution approach for preserving equity between users.

Recommendation: C7 is likely to improve performance and usability, although decreases confidentiality & integrity and availability. C8 enhances confidentiality & integrity, but suffers setback with usability, performance and availability issues.

Apart from the aforementioned four "quality" aspects, there are other considerations that designers should take into account, such as the economic cost. If a SNS is centralized, on the one hand, the SNS provider affords all economic costs to maintain the storage, communication, and development [NTB+12]. On the other hand, users that freely access the SNS services provide their personal data, which is used to generate revenue. Conversely, more decentralization of data and services trends towards a greater user participation in the SNS costs. In decentralized SNSs, each administrative domain partially supports the infrastructure costs for developing and hosting the overall system. In fully decentralized SNSs, each user maintains her portion of the SNS infrastructure. Table 4.3 table summarizes the positive (+) and negative (-) possible impact of decentralization of various combinations of privacy-related properties.

4.7 Limitations of the Contribution

In the multi-criteria analysis grid, privacy in SNSs is considered as a multidimensional composition of discrete properties rather than a single criterion. However, the main limitation of the analysis grid relies in not considering priorities when comparing privacy-related properties of distinct SNSs.

Lattice structures come along with their own set of operators, mathematical properties and algorithms. The limitation of the lattice structure adopted in this thesis is that it relies on basic comparison tools, which remain to be explored, adapted and integrated to the analysis of SNSs. Also, these basic comparison tools can be improved by the further integration of mathematical properties of algebraic lattice.

Moreover, an efficient manner is necessary to deal with the visual complexity to represent and manipulate the lattice structure, considering a large number of properties.

4.8 Conclusion

Currently, efforts engaged to protect users' data through decentralization of data and services in SNS aim at keeping the data with the users, on their personal devices, and at developing SNSs using PbD principles to overcome the issues raised by centralized control.

In this thesis, the position is to emphasize various design properties, which can be set at

Table 4.3 – Composition of properties

Qualities / Composition	Confidentiality & Integrity	Availability	Performance	Usability
C1. *Storage Space*(C) × *Replication*(C) × *Data Encryption*(FD)	+	-	-	-
C2. *Storage Space*(D) × *Replication*(D) × *Data Encryption*(FD)	+	+	-	-
C3. *Storage Space*(FD) × *Replication*(FD) × *Data Encryption*(FD)	+	+	-	-
C4. *Search*(C) × *Unlinkability*(C) × *Unobservability*(C) *P.A. Peer Policy*(C)	-	+	+	+
C5. *Search*(FD) × *Unlinkability*(FD) × *Unobservability*(FD) *P.A. Peer Policy*(FD)	+	-	-	-
C6. *Anonymity*(FD) *Pseudonymity*(FD)	probably incompatible			
C7. *P.E. Peer Policy*(C) × *Storage Space*(C) × *Retrieval*(C)	-	-	+	+
C8. *P.E. Peer Policy*(FD) × *Storage Space*(FD) × *Retrieval*(FD)	+	-	-	-

+: the positive impact on the quality
-: the negative impact on the quality

various degrees of decentralization, thus impacting the overall privacy level of the application. These properties are related to privacy issues, and have been organized in four groups: architectural services, storage, privacy policy management and security aspects of privacy. Based on the hypothesis that avoiding central authorities limit the risks of abuse, a multi-criteria analysis grid has been proposed to analyze and compare SNSs. The multi-criteria analysis grid, based on the degrees of decentralization, enables an accurate analysis to evaluate several properties of different SNSs. Then, the lattice theory was applied to this grid, allowing to build a comprehensive structure aimed at identifying which SNS performs better with respects to a given set of properties, and more generally at comparing SNS platforms in terms of privacy protection. Using the proposed lattice structure, it is possible to classify, evaluate and visualize different SNSs within a partial hierarchy, by using lattice chains and levels.

Both the multi-criteria analysis grid and the lattice structure developed in this thesis are contributions to PbD techniques, allowing SNS designers in the specification phase to distinguish best practices and to find out how to improve SNSs for the sake of privacy. Moreover, the identification of compositions and relationships between properties within the same group, as well as in distinct groups, provides new insights towards useful recommendations for designers of SNSs. These privacy-friendly techniques might be used to reduce developers efforts during the conception, planning and production of the SNS, by understanding the SNS characteristics and defining which property is the best to achieve a desired level of privacy, based on several design criteria.

Chapter 5

Equity-preserving Management of Privacy Policy Conflicts in SNSs

SNSs, such as Facebook or Twitter, have attracted many users since their foundation, mainly because they allow and encourage publishing and sharing interests, news, hobbies, activities and documents. Moreover, links can be made between documents and users by the means of *tagging*. The social relationships among users give semantics to these links, adding further value to this feature. In consequence, it happens that tagging is getting more attractive in SNSs in the last years [DJZ+09]. However, it also worsens existing privacy breaches by exposing user identities and providing further means to reach documents.

Although many attempts have been made to define privacy [Wes67], it is often based on the "right to be let alone" [WB90], associated with the "possibility to control the distribution and use of personal data" [Mül06]. This is usually implemented through the specification of individual privacy policies. When several users are entitled to a form of control over the same data (i.e., a picture of them as a group), conflicts may arise as soon as two of them disagree about the permitted usages of the document. When resolving conflicts, it appears that many strategies lead to unfair situations [SSP09], possibly allowing a few users to gain advantage over others if their policies are more frequently enforced.

In traditional human societies, the concept of equity is considered a basis for social justice and conflict resolution [Raw71]. In fact, this notion could be of help in SNSs as well. The second contribution of this thesis, described in this chapter, is a proposal of characterization of unfairness in the enforcement of privacy policies by introducing the concept of equity in SNSs. Then, a novel conflict management mechanism based on an algorithm designed to maintain or restore this equity is presented. The application of this equity-preserving algorithm may have a significant impact on the enforcement of access control, and therefore on data privacy. Putting a stress on equity may very well decrease the confidentiality of some resources, thus creating a trade-off with the classical view on privacy. Informed consent

is an important element to give users control over what other users may or may not access with respect to their personal data. Besides, users should be informed of the implications of a given consent. They should also be able to disagree about what data can be used for a particular purpose, or to revoke consent. These consent features are desirable options since they increase transparency and awareness in SNSs. In consequence, the output of such an equity-preserving algorithm should remain controlled and validated by users. For the experimentation purposes in this chapter, the consent decision is automatically taken by the proposed algorithm. However, in a deployed system it has to be done through an exception management system involving interaction with users. The second contribution of this thesis was first published at *The* 6^{th} *ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)* [MPB14].

The chapter is organized as follows. Section 5.1 presents an applicative context in which privacy conflicts may arise. In section 5.2, a notion of equity is proposed and the equity-preserving algorithm is presented. Section 5.3 describes the handling of consent in the equity-preserving algorithm. Section 5.4 compares the equity-preserving approach to some related works. Section 5.5 presents the limitations of the equity-preserving algorithm. Finally, some conclusion are presented in section 5.6.

5.1 Privacy Conflicts in SNSs

Information sharing is a core feature in SNSs. However, when more than two users have divergent privacy expectations to the shared data, privacy conflicts may rise.

5.1.1 Data Sharing in SNSs

SNS users share interests, news, hobbies, documents and activities. They can post notes and upload documents, like photos, on their web space, and tag friends in those documents. Most interactions between users and SNS resources occur in the form of tagging [GLYH11]: on Delicious, a user can assign tags to a particular bookmarked URL and have a personal set of tags per URL; on Flickr, users can tag photos uploaded by them or by others; on Blogger, Wordpress, Livejournal, blog authors can add tags to their posts; on Twitter, hashtags are used within the tweet text itself; on Youtube, multimedia objects like videos and music can also be tagged; on sites like MySpace, users can share large amount and different kinds of information and often annotate parts of the photos. On Facebook, when a data publisher tags her friends, the SNS sends a notification alert, after what the data subject can only accept the tag or not. If the data subject does not accept, the tag is removed and the data publisher cannot tag this data subject again. Studies have show that a majority of the users (75-80%) choose to approve the tag request [KLM+12, BRL10].

In general, tagging may relate to concepts like keywords describing a document, and is currently one of the most popular actions in SNSs [DJZ+09]. The tagging concept derives from the idea of organizing and sharing resources efficiently on the Web characterized by the principles of linked data[1] proposed by Sir Tim Berners-Lee [BHBL09]. Although in other

[1]Linked Data refers to publishing and connecting structured data on the web.

contexts people tagging may relate to non users, or be used for navigation, browsing, and for retrieving resources [DJZ+09], in this thesis tags are understood as links between documents and users.

In the context of data sharing and tagging, photo sharing is an activity that has increased drastically in social networking applications [BRL10]. Figure 5.1 represents a photo tagging context, in which users are classified as data publisher, data subjects and data viewers:

- The *Data Publisher* is the user who releases the data in the SNS (i.e., the picture is on her "wall");
- The *Data Subject* is a user to whom data is related (i.e., she is tagged in the picture);
- The *Data Viewer* is the user requesting access to the shared document.

The presented scenario consists in five users (Alice, Bob, Charlie, Greg and Eve) interacting within the same SNS. Alice uploads a document on her webspace. She becomes the *data publisher* for this document, in which she tags both Bob and Charlie. Therefore, Bob and Charlie are tagged in this document, hence becoming *data subjects*. Greg and Eve, may request access to the document, hence becoming *data viewers*. The scenario in Figure 5.1 will be the base for the present study, which focuses on access control issues with respect to privacy. Typically, in this kind of scenario the data publisher has more control than the data subjects about the collection and use of a shared personal data.

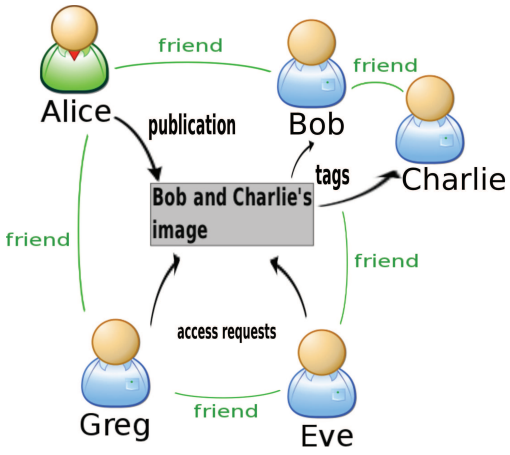

Figure 5.1 – The SNS scenario specification

5.1.2 Information Sharing Architecture

In many social networking frameworks, a centralized approach is used for performing some or all of the security features, like access control. In this case, there is usually a single *PDP* (as defined in section 3.2.6) to handle all data requests, and a single *PEP* (as defined in section 3.2.6) to implement the decision (and these points are often the same entity) [AW11].

Nonetheless, to cope with individual policies specified by each user, recent promising and efficient architectures tends to decentralize privacy policy management in SNSs [MPB13].

In the hypothesis of a decentralized architecture, one may imagine that a data publisher receives an access request and forwards it to the data subjects involved in the shared data. Here, it is considered that every user in the scenario described in in Figure 5.1 has an individual PDP. Each PDP decides whether the requester has the right to access the data or not, according to the user's privacy policy, and sends the user's ruling ("allow", "deny" or "do not care") to the *Decision Aggregation Point (DAP)*.

The DAP is the architectural component that manages a set of decisions, resolves conflicts according to a selected strategy, and generates the final access control decision. The DAP aggregates all decision rulings provided by the relevant PDPs, and thus is a centralized entity.

The decision of the DAP is sent to the PEP (possibly located where the data is stored, which may vary according to the SNS architecture), where the corresponding decision is enforced. If the decision is positive, the PEP grants access over data to the data viewer, otherwise, access is denied. Figure 5.2 depicts an overview of this architecture.

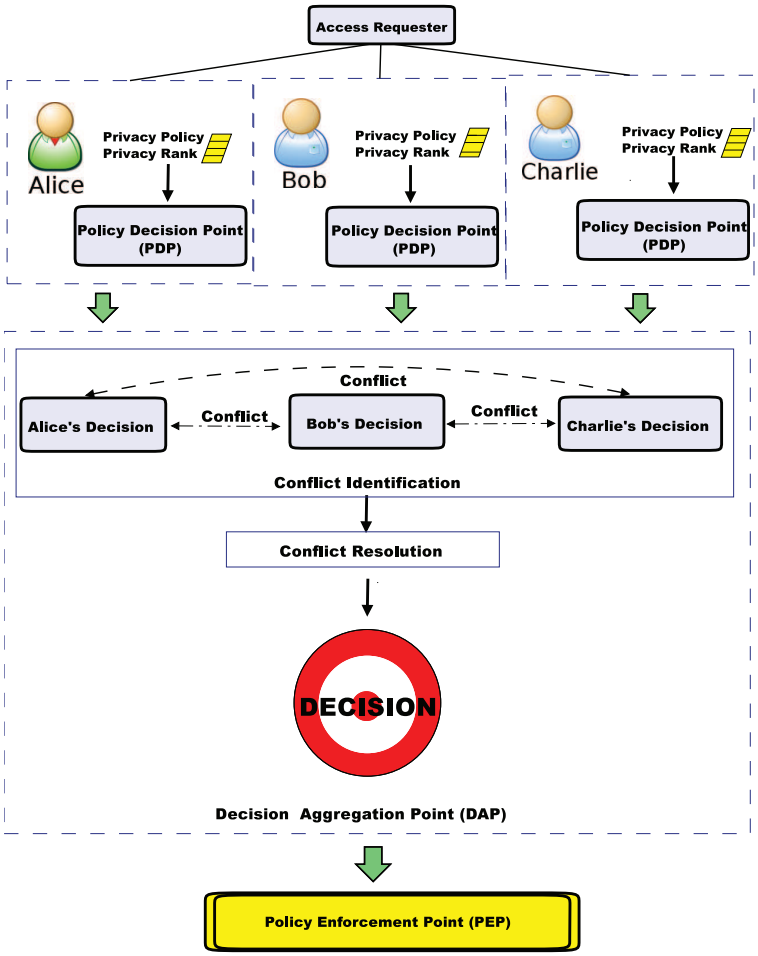

Figure 5.2 – Information sharing architecture

5.1.3 Expressing Privacy Policies in SNSs

Traditionally, SNSs publish system privacy policies that apply indistinctly to all users. In addition to those imposed policies, individual users are often given the opportunity to define their own policies, through a choice of settings and preferences (even though SNS providers may fail to properly enforce those user policies, or limit user empowerment through complex and abstruse privacy settings [ARG11]).

The users' privacy policies usually rely on access control rules, allowing users to define their sensitive assets and limit access to them. In most SNSs, only the data publisher has the right to define an access control policy over a published document.

Regarding the scenario presented in section 5.1.1, only Alice would be in position to decide who can access the picture she has uploaded, and neither Bob nor Charlie have anything to say about who can see the picture. Note that Bob and Charlie are in the photo and have no permission to control the related privacy settings, which may lead to privacy breaches for them. Moreover, even though the simple act of uploading a photo can represent a privacy violation, the fact that a person is publicly tagged in a picture can worsen the impact of the privacy breach, allowing other people to gain a searchable access to the user's identity.

To take this situation into account, data protection regulation frameworks often provide data subjects with rights to control the processing and disclosure of the documents relating to them [PtC95]. In the interest of privacy, any user tagged in a shared document should be able to define a privacy policy for it. In consequence, the scenario version presented in section 5.1.1 allows not only Alice (the data publisher), but also Bob and Charlie (the data subjects) to specify privacy policies when the document is published on Alice's webspace. For instance:

- Alice authorizes her "friends of friends" (including her friends) to be able to see the picture she publishes. All users in the scenario satisfy this condition;
- Bob has not defined a policy about pictures in which he is tagged, therefore not imposing any restrictions on anyone;
- Charlie authorizes only his direct friends to see a photo in which he is tagged. Therefore, Bob does satisfy Charlie's policy, while Alice, Greg and Eve do not.

The variety in privacy policies reflects the fact that SNS usages are spread over a broad dynamic range of different user profiles. Indeed, studies have shown that users often have rich and complex photo-sharing preferences [KLM+12]. To take this diversity into account, several privacy policy languages have been proposed, with various levels of expressivity [IW03, Org14]. For instance, in the EPAL language described in section 3.2.3, a user allowing people to gather her profile information for research purposes may impose that she is informed of every usage of this information.

Since every data publisher and data subject are allowed to express a privacy policy on a shared document, those policies may not be consistent with each other.

5.1.4 Conflict Resolution Strategies

The multiplicity and heterogeneity of these privacy policies may lead to conflicting situations, which occurs when at least two users disagree about the outcome of an access request[2]. Two approaches can be taken to tackle this issue. The first one would be to merge individual policies in a single policy decision point in charge of resolving the inconsistency. Many formalisms have been proposed for this, some of them specific to privacy policy composition [BDS04]. The second approach is to use an independent distributed policy decision point for each privacy policy, and to collect the rulings in a decision aggregation point in charge of resolving the conflicts, as depicted in section 5.1.2. In the second approach, the conflict is between rulings and not between policies. In this thesis, the second approach is chosen since it allows users to keep their privacy policies secret, and because it is expected the reasoning on rulings will be easier to design and lower in computational complexity.

The example in section 5.1.3 implies a conflict if Greg, for instance, requests access to the document: Alice allows, Bob does not care, and Charlie denies. Of course, Bob is not involved in the conflict, which takes place between Alice's "allow" and Charlie's "deny". Once the conflict is identified, a resolution strategy must be chosen to determine which ruling to enforce [JSSB97]. Different approaches exist to deal with conflict management and resolution, where the major ones are "deny strategy", " allow strategy" [JSSB97] and "majority strategy" [CCT07]:

- **Deny strategy**

  A common way to eliminate a conflict in access control is to use the *deny strategy*, in which a "deny" ruling is given priority over "allow" rulings. This strategy is usually chosen in most information systems, since it is considered a "secure" way of dealing with those situations. In the scenario described in section 5.1.1, Greg would be denied access because of Charlie's ruling.

- **Allow strategy**

  In *allow strategy*, an "allow" ruling is given priority over "deny" rulings. In the scenario described in section 5.1.1, Greg would be granted access due to Alice's ruling. It can be noted that in most SNSs, allow strategy is the standard choice when resolving policy conflicts [YKP12].

- **Majority strategy**

  Another approach for deciding among multiple alternatives is to vote. The *majority strategy* gives priority to the ruling supported by the majority of users. In the scenario described in section 5.1.1, if Bob changes his mind and allows only his direct friends to access pictures in which he is tagged, he will issue a "deny" ruling for Greg. Greg would thus be denied access due to a majority of deny decisions.

Although Deny, Allow and Majority strategies are mentioned in this thesis, other more exotic examples of strategies such as "preference strategy" and "default strategy" exist [CCT07].

[2]It can be noted that a single policy may be self-conflicting when it includes inconsistent rules, but this issue lies outside the scope of this thesis.

The *preference strategy* gives priority to the ruling determined by the data publisher. In the scenario described in section 5.1.1, Greg would be granted access due to Alice's ruling, because she is the data publisher. *The default strategy* is applied when other resolution strategies are not conclusive, for instance when involved users do not provide any ruling. This strategy gives priority to the more adapted ruling in the context (e.g., "deny" ruling are preferred in security and privacy systems). In the scenario described in section 5.1.1, if Alice, Bob or Charlie have not defined any ruling and considering a SNS where privacy is relevant, the default ruling should probably be "deny". Then, Greg would be denied access. A *strategy based on social graph topology* can also be designed, by using the distance between the data subject issuing the ruling and the data publisher. Due to the fact that *social graph strategy* and *preference strategy* introduce priorities between data publisher and data subjects, options such as *default strategy* may boil down to deny strategy. *Social graph strategy* and *preference strategy* impose a tradeoff between various rights, namely the data subjects' right to control their image, the putative photographer's copyright and the usage rights commonly attributed to the data publisher in SNSs.

All the strategies stated above can be used to resolve policy conflicts. Unfortunately, these strategies make decisions in a very static way, possibly allowing some users to take advantage over others. For instance, the classical deny strategy allows a user to prevent anyone from seeing any picture of her. Such a constant and systematic opposition can, in the long run, be considered highly unfair to other users because their privacy policy may never be enforced. In this thesis a more dynamic resolution strategy, that can overcome this limitation, is proposed.

5.2 Equity Approach to Conflict Management

Conflicts arise because people do not consistently agree about their privacy preferences. When the demands or desires of one part are in conflict with others, conflict resolution strategies generally try to achieve an effective resolution. However, a user can find that these strategies induced unfair decision making, generating deceptive behaviour and violations of her privacy rights. To characterize this issue in a more clear and objective way, the notion of *equity*[3] is introduced to encompass the intuitive fairness or unfairness of a situation.

5.2.1 The Notion of Equity

The original meaning of equity arises from the Greek word *epieikeia*: a sort of justice. Indeed, this concept is inherited from the Greek civil legal system, which was originally defined by Aristotle: on the one hand, in the *Ethics, Book V*, equity emphasizes the moral virtue that represents the exercise of making equitable judgement [Shi94]; on the other hand, in his work called *Rhetoric*, equity helps to preserve the authority of the law by correcting its unjust application [MS14]:

[3]Aiming to introduce a new notion in this field of study, it was decided to not use the term "fairness", which already has a specific meaning in several subfields of computer science.

"For that which is equitable seems to be just, and equity is justice that goes beyond the written law. And it is equitable to prefer arbitration to the law court, for the arbitrator keeps equity in view, whereas the judge looks only to the law, and the reason why arbitrators were appointed was that equity might prevail."

The notions of equity in the *Ethics* and in the *Rhetoric* are the ones commonly cited as the source for the Latin word "*aequitas*", and the ultimate source of the English word "equity" [MS14].

Equity is not a unified concept and has many meanings depending on the context: political, philosophical, legal, societal or economical. The first distinction is between equity and equality. The *Oxford English Dictionary*[4] defines the term "equity" as the quality of being fair and impartial, whereas the term "equality" corresponds to the state of being the same in quantity, size, degree or value. These definitions show that in human affairs, equity is not necessarily the same as equality, in the sense that giving the same amount to different people, in different contexts, can be deemed unfair. The abstract notion of equity is understood by most people in terms of social value (i.e., social welfare). This chapter, stemming from the users' perception of the situation, focuses on equity rather than equality, even though equality may prove a useful tool for building equity.

Equity, as a taxation concept, is used in two dimensions: horizontal and vertical. Horizontal equity refers to the notion that equally situated individuals in economic terms should be taxed equally, whereas vertical equity refers to the notion that differently situated individuals in economic terms should be taxed differently in a way that society deems to be fair [BB11]. In legal terms, the role of equity was developed alongside common law in order to control the unconscionable assertion of one's strict legal rights [Kea10].

In the socio-economic context, due to the difficulty in achieving social justice and redistributing available resources in our society, Hayek [Hay73] believes that social justice is but a dream out of society's reach. However, Rawls [Raw71] defends equity as an ethical concept of justice or fairness, being the base of a society that cooperates and shares its benefits and burdens, thus creating a surplus which should be fairly distributed. In this context, social equity means a balance in the distribution of benefits constructed by society, such as electricity, drinking water, and public transportation. According to other opinions, in the context of public health, the concept of equity is closely related to human rights principles [BC03]. The latter reference interprets equity as the absence of systematic disparities in health among groups, highlighting social advantages and disadvantages. These notions are related to the issue of equity in this thesis, in the sense that they reason on situations where individual interests are conflicting and an acceptable solution must be reached.

5.2.1.1 Defining Equity in SNSs

The notion of equity in SNSs has to be characterized, such as in the special case of the scenario described in section 5.1.1. Suppose, on the one hand, that Alice and Bob authorize only their friends to see the picture and, on the other hand, that Charlie has specified in his policy an interdiction, stating that nobody should be able to see the photos in which

[4] http://www.oxforddictionaries.com/

he appears. If the "deny strategy" is applied, the situation is somewhat unbalanced, as described at the end of the section 5.1.3: Charlie always gets what he wants, while Alice and Bob never get it. This situation is inequitable because Charlie sees its preferences prevailing over others', in the form of a more frequent enforcement of the policy he has chosen. In the light of this example, equity in the context of SNSs can be defined as follows:

Definition 1 *In the context of a Social Network System, a situation is said to be* ***equitable*** *if and only if all considered participants have seen their policies enforced or violated in the same proportion over past interactions.*

In the event of an inequitable situation, the SNS may try to restore equity by introducing some kind of restoration of equity when resolving privacy conflicts, by influencing the enforcement of user policies. It should be noted that in this perspective, the objective of achieving perfect equity may become conflictual with the quest for the highest possible level of confidentiality. In other words, although equity, in this context, is closely linked to privacy, the two concepts do not necessarily concur. In the next section, a management mechanism and the development of an equity-preserving algorithm is proposed to tackle the issue of equitable enforcement of multiple user policies in SNSs.

5.2.2 An Equity-preserving Conflict Management Algorithm

Users specify their privacy policies according to their privacy concerns and preferences regarding shared data. A privacy policies is composed of a set of rules, which are used to regulate how much information is allowed to be shared, and determine who is allowed to know the information. These rules impact the management of individual and collective privacy boundaries. Individual privacy rules are based on cultural values, gendered orientations, and personal motivations. However, when a private information becomes shared, a collective privacy boundary is formed, yielding a jointly control of that information [Pet02]. Rules can lead to three types of ruling: *allow*, *deny* and *do not care*. The ruling "do not care" is not an enforceable ruling: it allows more flexibility and expressivity, while being compatible with rich privacy policy languages such as EPAL [IW03]. In a privacy policy composition context, the "do not care" ruling can simplify the combination of different policies, when each policy only covers a given scope [BPS03].

The proposed algorithm here starts when a data viewer submits a request to access a document published by a data publisher. The algorithm is composed by some metrics on users, applied in order to analyse the enforcement of policies in the SNS, namely: Number of times one's Policy has been Violated (NPV), Number of times one's Policy has been Enforced (NPE), and Number of Interactions (NI). If no conflict is detected, all the relevant rulings are the same (e.g., either *allow* or *deny*). Then, the conflict detection algorithm should return a "no conflict" answer. In this case, the consensual ruling is enforced and the metrics are updated (in this case, NPV is not incremented).

A conflict arises when rulings are not compatible. Once all the necessary user rulings are collected, the algorithm identifies whether there is a conflict among them. It is worth

noting that the conflict detection algorithm only detect conflicts among rulings, and does not consider condition or obligation elements. In case of a conflict, then the equity conflict resolution algorithm is run.

Figure 5.3 presents the equity-preserving conflict management algorithm. The approach relies on three main steps: an equity evaluation (labelled A), a compensation phase (labelled B) and an additional prioritization based on user preferences (labelled C).

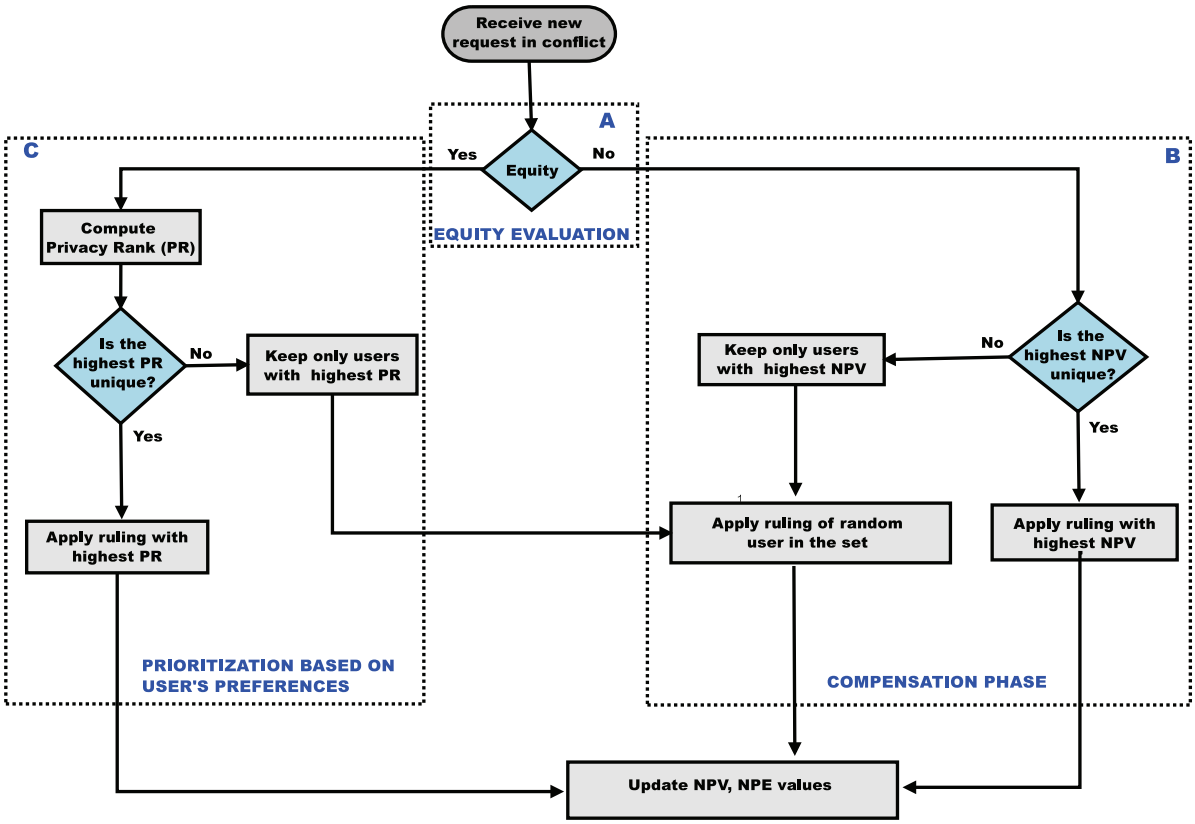

Figure 5.3 – The equity-preserving conflict management algorithm

5.2.2.1 Equity Evaluation

In Figure 5.3, the first step "A" is called *equity evaluation*. It determines whether the current situation is equitable, according to the definition in section 5.2.1.1. For that, the algorithm needs to measure the number of times a given user has seen her policy rejected for enforcement (NPV) and the number of times this same user has been involved in an access request (NI), as described in Algorithm 5.1. Note that even in the absence of a conflict, each user's NI is updated each time she is involved in an access request. The ratio between NPV and NI (a "normalized" NPV) is the proportion the equity decision is based on. It actually measures the proportion with which a user has seen her policy denied, and not enforced.

One of the most discussed criteria of equity is *proportionality* [LRS98]. The Aristotelian

Algorithm 5.1 Equity evaluation algorithm

Input: list of users in conflict (usersInConflict)
Output: *boolean equity*

```
1: i ← 0
2: while usersInConflict[i+1] exists do
3:    currentNPV ← normalizeNPV(usersInConflict[i])
4:    nextNPV ← normalizeNPV(usersInConflict[i+1])
5:    if currentNPV != nextNPV then
6:       return false
7:    else
8:       i ← i + 1
9:    end if
10: end while
11: return true
```

criterion of justice as proportionality is represented by the equality of ratios (proportion) between two parties [Eng12, Eng13]. Under a similar assumption, a simple equality test over the normalized NPVs of all users involved in the conflict was chosen in this thesis as equity evaluation[5].

If the equity evaluation result is false, the situation is deemed inequitable according to the definition in section 5.2.1.1, because all users have not had the same proportion of policy violation, actually in the past. The SNS then tries to restore equity, and a *compensation phase*, labelled "B" in Figure 5.3, begins.

5.2.2.2 Compensation Phase

Generally, inequity produces a negative emotional state which generates social tensions, crime, and similar problems [Ben00]. One way to reduce a user's distress is to restore equity through the reestablishment of benefits. The compensation phase will favour a user who has the highest normalized NPV, in order to lower this value for her and restore some equity, as described in Algorithm 5.2.

At this point, the algorithm checks whether the highest NPV is unique among the users in conflict (therefore excluding the ones having sent a "do not care" ruling). If there is a single user with the highest NPV, then the algorithm will enforce her ruling. When this decision is taken, all users having sent the winning ruling will see their (NPE) incremented, all users having sent the losing ruling will see their NPV incremented. The NI of all users is also incremented.

If the highest normalized NPV is not unique, then the algorithm will keep the set of users with the highest normalized NPV and proceeds to the last step of the compensation phase, randomly chosen a user in the remaining set of highest normalized NPV and elect her ruling for enforcement. Once the ruling is chosen, all counters are updated as previously described.

[5]The possible implementations of equity were broader tested during the development of this thesis, allowing little differences between normalized NPVs, but tests have shown that strict equality leads to far better results.

Algorithm 5.2 Compensation phase algorithm

Input: list of users in conflict (*usersInConflict*)
Output: *list of ruling*

```
1:  int i ← 0
2:  int maxNPV ← 0
3:  highestNPV ← emptyList()
4:  highestNPV.add(usersInConflict[i])
5:  while usersInConflict[i+1] exists do
6:    maxNPV ← normalizeNPV(highestNPV.get(0))
7:    nextNPV ← normalizeNPV(usersInConflict[i+1])
8:    if nextNPV > maxNPV then
9:      highestNPV.clear()
10:     highestNPV.add(usersInConflict[i+1])
11:   else if nextNPV = maxNPV then
12:     highestNPV.add(usersInConflict[i+1])
13:   end if
14:   i ← i + 1
15: end while
```

5.2.2.3 Prioritization Based on User Preferences

If at the equity evaluation ("A") phase of the algorithm the situation is deemed equitable, then the branch "C" is taken, such as described in the Figure 5.3. Then, the final ruling decision must be made based on different criteria. Here, the proposed process intends to take into account the users' preferences and evaluations in terms of privacy, since this is the overall goal of the application. Different works have been proposed to measure the privacy risk using the sensitivity of the information to be revealed and the visibility of profile attributes in the SNS [WN13, LT10]. In this thesis, privacy concerns expressed by the users are ordered, in the form of a *Privacy Rank (PR)*. From the technical point of view, a definition for PR should satisfy the following properties:

- The higher the privacy risk[6] associated to the data, the higher the PR. The variable that embeds this notion, is called *Data Value (DV)*. DV defines the sensitivity associated to a resource. Different users may have different privacy concerns regarding a same piece of information. A classification in five levels of DV rated on a Likert scale [Lik32] are proposed in this thesis: 5 - extremely sensitive, 4 - very sensitive, 3 - sensitive, 2 - hardly sensitive, and 1 - not sensitive;

- The higher the risk associated to a particular access request, the higher the PR. The variable that embeds this notion, is called *Rule Value (RV)*. RV defines the importance of a specific rule within a user's policy. Rules may be marked as important when there is the necessity of a *strong allow* or a *strong deny*. Less important rules boil down

[6]It is worth noting that the term risk is often used in different domains, such as risk assignment, with different interpretations. In this thesis, risk is an indicator of potential threat to user privacy.

to *weak denies* or *weak allows*. Similarly to DV, RV has five levels rated on a Likert scale [Lik32]: 5 - extremely important, 4 - very important, 3 - important, 2 - hardly important, and 1 - not important.

The chosen implementation defines PR as a product of both DV and RV, which ensures the desired properties in a simple way:

$$PR = DV \times RV,$$

However many other combinations could be defined.

While the need of a "strong deny" is pretty obvious, it is also important to allow a user to express her need for the availability and publicity of a particular piece of information. Although this does not specifically increase any confidentiality level, it contributes to a higher control of the user over her information, a better user centring of the application and probably a more operational notion of free speech. In the context of the scenario described in section 5.1.1, let us suppose that Alice becomes the new director in the company where Bob and Charlie are employed. Alice wants all employees to know who the new director is. Therefore, her ruling on this information is an "allow" and the associated rule value is set at level 4 or 5 (this is a "strong allow"), while the data value will be low, the information being somewhat public already. In another contrasting example, let's assume that Alice authorizes her direct friends to see her wedding picture. The data value of this document is pretty high, since it may have a strong impact on the privacy of her family life. The rule value of the associated "allow" rule will be rather low if she thinks that it is not vital for her friends to see this picture, but the rule value of a "deny" regarding strangers would be quite high.

If the algorithm finds a unique highest PR, the corresponding ruling will be given priority and therefore enforced (and the metrics updated). If the highest PR is not unique, then the set of users with highest PR is kept and the algorithm switches to the last part of the compensation phase, with a random selection of the ruling in the remaining set of highest-PR users, as described in Algorithm 5.3. One may notice that the PR is only used when the initial situation is equitable. Thus, the resulting algorithm gives priority to equity between users over privacy ranks defined by users. It is worth noting that PR could be subject to discussion, but the main goal is to show that the notion of equity can be integrated to the conflict resolution, even in the presence of other considerations.

5.3 Consent

In real world applications, consent may decrease the usability of systems like SNSs, depending on how it is implemented. Systematically asking for an explicit consent for each and every access request is of course an inacceptable burden. However, relying too much on opt-in/opt-out systems[7] leads to blanket rulings, not necessarily reflecting the users' preferences. The limited effectivity of the trade-off chosen by Facebook is a telling example of this issue.

[7]Opt-in refers to a situation in which a user needs to specify when she grants consent. Conversely, opt-out refers to a situation in which a user needs to specify when she declines consent.

Algorithm 5.3 Prioritization Based on User Preferences Algorithm

Input: list of users in conflict (*usersInConflict*)
Output: *list of ruling*

```
1:  int i ← 0
2:  int maxPR ← 0
3:  highestPR ← emptyList()
4:  highestPR.add(usersInConflict[i])
5:  while usersInConflict[i+1] exists do
6:    maxPR ← getPR(highestPR.get(0))
7:    nextPR ← getPR(usersInConflict[i+1])
8:    if nextPR > maxPR then
9:      highestPR.clear()
10:     highestPR.add(usersInConflict[i+1])
11:   else if nextPR = maxPR then
12:     highestPR.add(usersInConflict[i+1])
13:   end if
14:   i ← i + 1
15: end while
```

Of course, consent provides benefits by better meeting the expectations of users for direct control over data. In essence, the key of this control involves the user's decision determining how her information may be used and disclosed. Typically, consent is identified by focusing on key words, such as opt-in and opt-out. For instance, in P3P (described in section 3.2.3) the use of opt-in or opt-out options refer to the user's consent regarding the disclosure of her private data.

The algorithm, as it is presented, takes automated decisions about the violation of user access control policies, without any control from users. This is acceptable in an abstract intellectual exercice, but of course not in production systems, which need to comply with usual data protection regulations. In consequence, it is absolutely necessary to take user consent into account when integrating the equity algorithm previously presented in section 5.2.2 to regulate the control over access to user personal data. Instead of automatically enforcing the elected privacy policy for a given access request, the equity algorithm should request consent to users that have policies about to be violated. To manage consent in this context, two approaches can be taken. The first one would be to propose the users to update their policies in order to modify rulings that are not compatible with the policy elected for enforcement. After a consensual agreement among rulings appears, the conflict disappears and the user's NPE is updated while her NPV is not updated. The second approach is through the management of exceptions to privacy policies. In such a case, users whose ruling are incompatible with the policy elected for enforcement may agree to concede exceptions and punctually alter their ruling. In this case, the conflict remains, which implies an update of the metrics (NPE and NPV). The scenario in section 5.1.3 can be used to illustrate the consent handling. In the scenario example, Greg requests access to the document, which Alice allows but Charlie denies. Let us suppose that Alice's policy is elected for enforcement.

Then, applying the first approach suggests that Charlie's ruling could be transformed in an allowing ruling if he chooses to alter his policy. Otherwise, applying the second approach suggests that Charlie's ruling remains a deny ruling, but he accepts the arbitration of the algorithm.

5.4 Related Works

The equity-preserving algorithm proposed in this chapter is an original contribution that provides and integrates the concept of equity in the field of policy conflict management, and in particular in the context of privacy policies. No other equity-preserving algorithm designed to tackle the issue of equitable enforcement of multiple user policies in SNSs could be found in the existing literature.

However other concepts presented in this thesis, are far from new and can be found in several studies. In 2011, Hu et al. [HAJ11] have proposed a conflict resolution strategy based on the quantification of privacy risk and losses in potential data sharing from multiple users, in the context of a collaborative data sharing SNS. To address this issue, every *data controller* (i.e., every user issuing a policy over the shared data) defines a set of *trusted users* who can legitimately access the data. Any requester then needs to be a trusted user for all data controllers in order to access a content. This approach actually boils down to a strict implementation of the deny strategy. In fact, this approach is too static, since friend behaviour change over time, and friendship links can be broken and re-created. The approach presented in this thesis is believed to be more robust and flexible than this specific resolution strategy, since it is not built upon fixed trust relationships.

Squicciarini et al. [SSP09] focus on the collaborative management of privacy settings for shared content by using game theory. Mainly, the Clarke-Tax mechanism[8] promotes a collective policy that aggregates all individuals preferences into a single representative group. The expressiveness of this model depends on the users' understanding of the Clarke-Tax mechanism, which significantly reduces its usability. The current thesis presents a very different approach, in which users are not encouraged to reveal their preferences in the form of privacy policies, allowing those policies to be fully dynamic, evolutive, context-dependent and even not fully consistent, depending on how users choose to manage them.

5.5 Limitations

In democratic societies, the right to privacy is generally asserted by law or even higher principles, like Human Rights. It also seems necessary to strive for a better equity among individuals, as a consequence of equality rights and because it is seen as a desirable societal and political property. While traditional conceptions of privacy are related to secrecy, intimacy, limited access to information, and control over personal information, Solove [Sol12] advocates that privacy is a broader term which reveals influences of many other essential human conceptions including freedom, social welfare, individual well-being, which collectively

[8] The Clarke-Tax mechanism is an utility-based social choice mechanism that encourages truthfulness among individuals, regardless of other individuals choices.

do not reflect a single conception of privacy. Solove's new approach emphasizes privacy as a societal interest, not just an individual right.

Similarly, some equity theorists such as Austin and Walster [AW74] have proposed and demonstrated that societal equity with others in general prevails over equity with a specific person, in cases when both behaviours cannot be displayed together. Equity and privacy theorists assume that the collective interest rather than individual expectations governs human society, but an open challenge is to find ways to properly balance societal equity and individual privacy.

The equity-preserving algorithm described in this chapter solves conflicts while improving equity in the SNS. The resolution of privacy policy conflicts between autonomous entities is made by a non-deterministic choice, allowing to have different privacy policies enforced each time over the same shared data while keeping equity within the SNS in general. As a consequence, this situation leads to larger disclosure of users' personal data. It is worth noting that the proposed algorithm does not ensure a better confidentiality of secret information, from the privacy point of view. However, users are able to enforce availability policies on their data as a way to increase control (i.e., individuals can freely determine what is necessary and desirable in terms of privacy policy). This idea of privacy as control is expressed in Westin's classic definition of privacy in 1967 [Wes67], as quoted in chapter 1.

One possible solution to balance privacy and equity could be an improvement of the current equity-preserving algorithm. More precisely, the current equity evaluation considers that equity exists if normalized NPVs are equal. In other words, equity states fairness as a ratio (proportion) among parties. If the equity evaluation phase is modified to take into account the PR value, disclosure of information might be minimized. The remaining open question is therefore to determine how to integrate the PR in the equity evaluation.

5.6 Conclusion

This chapter examines the issue of handling conflicting privacy policies in the context of SNSs. Traditional conflict resolution strategies often lead to inequities among users, some of them being able to see their policies enforced more often than other. A new, equity-preserving resolution strategy is proposed, which does not require negotiation or mutual agreement among users regarding their privacy preferences.

The equity concept, when applied to SNSs, implies in the equal proportion of users' policies enforcement or violation. The equitable enforcement of multiple users' policies in SNSs is, in principle, a fundamental and necessary condition to establish fair decisions over privacy settings. Using the equity-preserving strategy presented in this chapter, users are encouraged to not cheat about their privacy concerns through the manipulation of their PRs. In other words, manipulating the true value of the users' PRs will not provide benefits, because inequities are balanced during the compensation phase of the equity-preserving algorithm. Nevertheless, in practice, the proposed algorithm does not ensure that users' preferences are truthful.

The proposed equity-preserving conflict resolution strategy has a broader application domain. Obviously, this strategy can be applied to other kinds of security policy conflicts

(and surely enough, it was only used with very simple privacy policy rules as examples). It is also believed, in this thesis, that this kind of algorithm can be of use in many multi-party decision taking scenarios in multi-agent systems, even outside the normative context. Moreover, the conflict resolution strategy would be particularly useful in small agent societies, in which local inequalities cannot be compensated by the statistical expectations of a large number of interactions over a large number of entities.

The proposed equity-preserving conflict resolution strategy implementation and experimental results will be explored in the following chapter.

Chapter 6

Implementation and Evaluation of the Equity-preserving Conflict Management Algorithm

The primary focus of the equity-preserving conflict management algorithm described in chapter 5 is to enhance equity in SNSs. In order to determine if the proposed algorithm actually reduces inequity, the first need is the use of an appropriate metric to measure equity. Then, the equity-preserving algorithm can be compared with other policy conflict resolution strategies (i.e., deny, allow and majority).

This chapter is organized as follows. Section 6.1 explains the Gini coefficient, metric used to evaluate the equitability of the equity-preserving algorithm. Section 6.2 introduces the implementation and a functional description of the prototype. Section 6.3 exposes the configuration parameters of the scenarios through empirical experimentation, and discusses the results. Section 6.4 presents the limitations of the implementation. Section 6.5 concludes the chapter.

The results presented in this chapter have been published at *The* 6^{th} *ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)* [MPB14].

6.1 Measuring Equity

Different measurements have been proposed to examine the fair distribution of a resource, such as the Atkinson index [Atk70], the Theil index [The67], and the Gini Coefficient [Gin12]. While there is no agreement on what is the best measurement for equity, the Gini Coefficient is the most commonly accepted.

The Gini coefficient is a classic tool and has been used in several works with more than thirteen alternative representations [CV12]. Originally designed in the field of economics to

measure various kinds of inequities in the society (e.g., the distribution of wealth or income over a population) [Gin12], the Gini coefficient became well known after the 2008 financial crisis and has since then contributed in exposing to the general public the income inequities in our societies. Nowadays, the Gini coefficient is a metric not only used to characterize inequity in economics, but also applied to other fields of knowledge such as in biology (e.g., to describe the distribution of plant size) [WS84, SB04], genetics (e.g., to assess the inequity of the genetic variability) [GPET03], astronomy (e.g., to quantify the distribution of galaxies) [AvdBN03], and SNSs (e.g., to study how the structure of a network and its dynamics affect social welfare and inequity) [NCM13, LCM13].

The terms "equity" and "equality" are usually mentioned in the context of income distribution, when the Gini coefficient is mentioned. By definition, while equality suggests equal share, equity is related to fair share [BC03]. Several equity theorists agree that equity implies equality, even though there is no consensus concerning on what should be equal [Cul01]. According to the definition in section 5.2.1.1 of this thesis, equality is a component of equity. Thus, equity concerning policies enforcement should refer to an equal proportion of enforcement or violation over past interactions.

The Gini coefficient measures the degree of inequity of the distribution of a resource in a population. It allows direct comparison with different size populations [THZZ14]. Moreover, the Gini coefficient may be used to decompose inequity in population subgroups, in cases where the resources can be organized in ascending order and non-overlapping sub-resources [Cow09]. So, if inequity increases for each population subgroup, then overall inequity also increases.

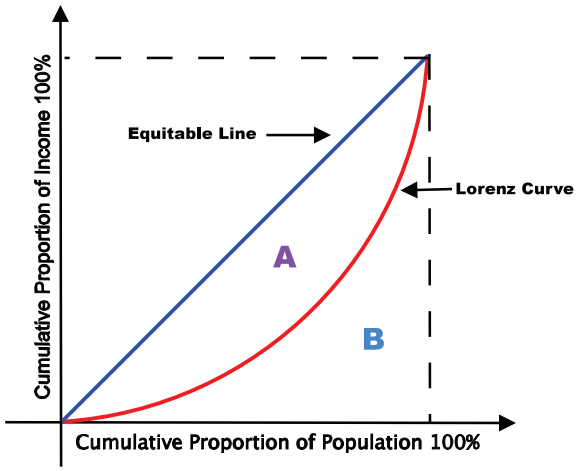

Figure 6.1 – Graphical representation of the Gini coefficient

The Gini coefficient ranges from 0 (perfect uniform equity) to 1 (perfect inequity), where smaller coefficients indicates a lower disparity in the distribution. It is easy to calculate [Cha90], and has a direct graphical interpretation representation based on the Lorenz curve (a Lorenz curve represents the cumulative distribution of quantity over a population) [WZS+12]: the Gini coefficient is defined as a ratio between the areas of two Lorenz curves. Figure 6.1 represents the two Lorentz curves. The blue curve represents the equity diagonal and is the

one of a perfectly equitable distribution, which boils down to the identity function. This equitable line represents the situation in which a resource is distributed equally (i.e., the poorest 10% would earn 10% of the total resource) [YS13]. The red curve represents the actual distribution (a necessarily convex function on $[0, 1]$). If the area between the line of perfect equity and the actual Lorenz curve is A, and the area under the actual Lorenz curve is B, then the Gini coefficient is A/(A+B).

In this thesis, the Gini coefficient was chosen as a metric to measure the resulting degree of inequity in SNSs, and to evaluate the efficiency of the equity-preserving algorithm compared to other conflicting resolution strategies. During the investigation performed in this thesis, no other research work using this coefficient to measure inequities of the enforcement of privacy policies was found.

In this thesis, Brown's equation [Bro94] was adopted since it is appropriate for discrete distributions in which only values at certain intervals are given, and is described as

$$G = 1 - \sum_{i=0}^{k-1} (Y_{i+1} + Y_i)(X_{i+1} - X_i) \tag{6.1}$$

where k is the number of users in the population, Y_i is the cumulative proportion of the resource up to user i, and X_i is the cumulative proportion of the population up to user i (Figure 6.2).

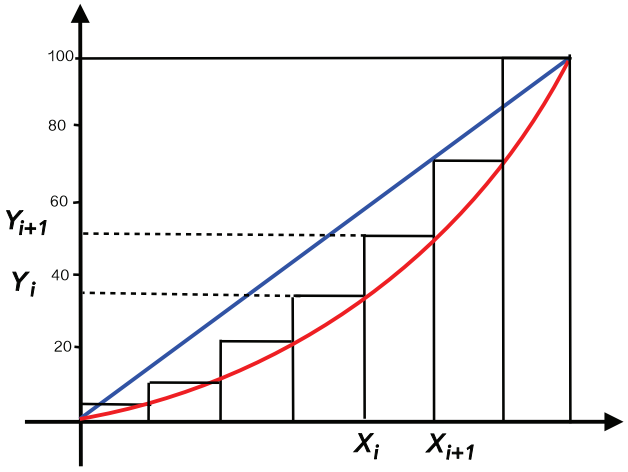

Figure 6.2 – Graphical representation of the Gini coefficient

The Gini coefficient is applicable to any quantitative attribute that can be redistributed among units of a given population, such as income, taxes, wealth, profits and losses [RSV14]. Following this definition, the metric that embeds the notion of profits in the equity algorithm is NPE (Number of time one's Policy has been Enforced, see section 5.2.2, page 131), which measures the user's policy enforcement. Also, the metric that embeds the notion of losses in the equity algorithm is NPV (Number of time one's Policy has been Violated, see section 5.2.2, page 131), which measures the user's policy violation. Thus, inspired on a typical economic analysis that measures inequity based on the evaluation of income and wealth distribution,

the Gini coefficient could be calculated using the ratio NPE/NI as the distributed resource to measure the inequity relation to policy enforcement, or the ratio NPV/NI of considering policy violation. A manner of relating these two metrics and find out which one present the highest inequity is through the computation of the maximal value between them. Thus, the Gini coefficient is calculated using the ratio $max(NPE, NPV)/NI$.

In this thesis, Y_i is the cumulative proportion of the resource up to user i such as NPE/NI and $max(NPE, NPV)/NI$, and X_i is the cumulative proportion of the population up to user i (that is, $X_i = i + 1$).

$$Y_i = \sum_{j=0}^{i} \frac{NPE_j}{NI_j} \quad \text{or} \quad Y_i = \sum_{j=0}^{i} max\left(\frac{NPE_j, NPV_j}{NI_j}\right) \tag{6.2}$$

6.2 Prototype Implementation

The equity-preserving conflict management prototype has been implemented in Java, and consists in 36 files and 8,518 lines of code. Experiments are conducted using an Apple MacBook Pro with the following configuration: Intel Core i7 (2,4 GHz) with 4GB of RAM, running a OS X operating system version 10.9.5. For explicitness, the functional aspects of the application are depicted in Figure 6.3 using a Unified Modeling Language (UML) class diagram. In this Figure, the *User* class represents the users in the SNS, the *Policy* class represents the users privacy policies, the *Rule* class represents the rules of the privacy policies, the *Data* class represents the set of resources of a given user, and the *Tag* class represents the links between a given resource and a set of users (i.e., the users that have been tagged for that resource).

The prototype offers four main functions, as presented below:

- **The specification of privacy policy rulings** that allows the users to specify their privacy policy for each resource they upload. More specifically, when a user uploads a resource on her webspace (she becomes the data publisher of that resource), she also specifies a privacy policy for that resource. She defines the data value level (*extremely sensitive*, *very sensitive*, *sensitive*, *hardly sensitive*, or *not sensitive*) associated with that resource. Then, she specifies a rule value level (*extremely important*, *very important*, *important*, *hardly important*, or *not important*) defining the importance of a specific rule associated with a particular access request, and a ruling decision option (*allow*, *deny* or *do not care*) is set according to her privacy concerns and preferences regarding that specific resource. Hence, a privacy rank is calculated. In summary, the user sets up her privacy options for the published resource (data value level, rule value level, privacy rank and ruling), authorizing her friends of friends to see the resource she published.

- **The tagging resource** that allows the users to tag the resources and the tagged users to specify their privacy policy for each resource in which they are tagged. Suppose that the user Alice tags the users Bob and Charlie in a given resource. They become the data subjects of that resource, and as such, they are notified about the tagging made by Alice. It is worth noting that the same privacy options (data value level, rule value

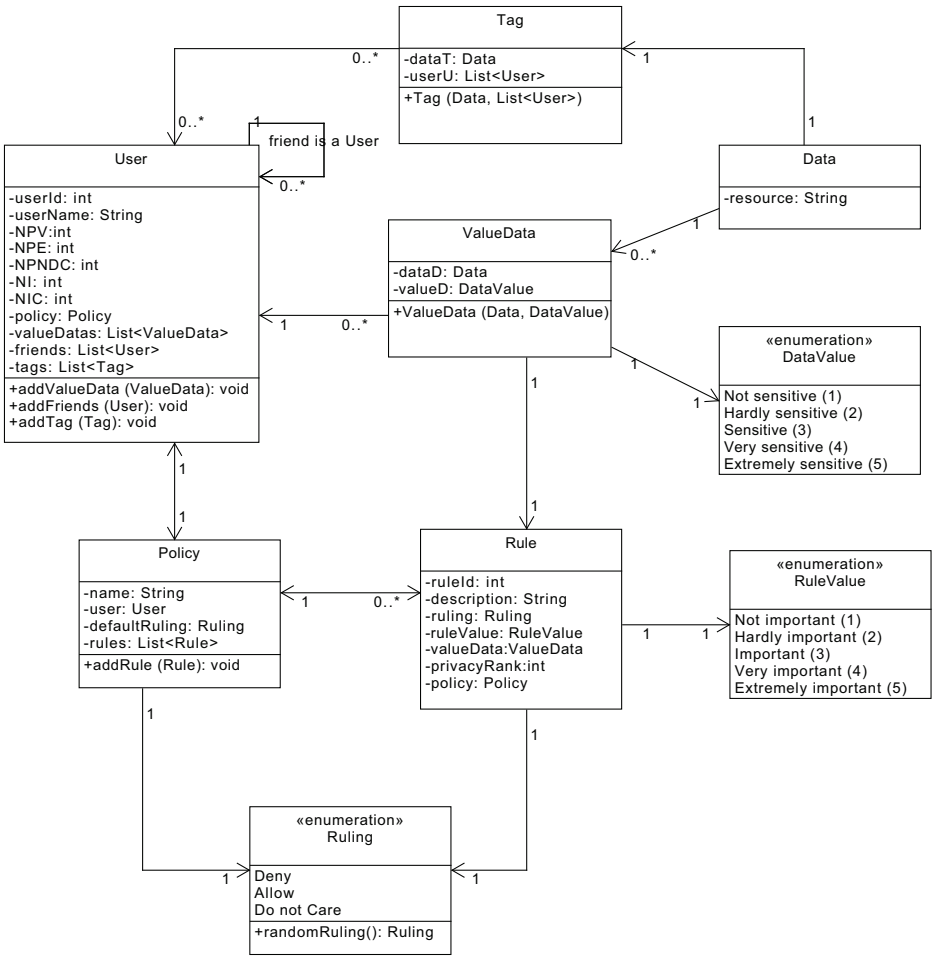

Figure 6.3 – Implementation of equity-preserving algorithm

level, privacy rank and ruling option) are also applicable to each data subject when specifying privacy policy in resources in which they are tagged. Thus, as previously, Charlie and Bob set up their own privacy policy for that resource. As a result, the shared resource is associated with rules generated by the data publisher and the data subjects.

- **The access request** that allows the users to request access to the resources published in the SNS. Let us suppose a user requests an access to a given resource. At this point, both the data publisher and the data subjects have set their policies, specifying their privacy options. For each access request, the privacy policies of the data publisher and the data subjects are individually evaluated, and each user's ruling is sent to the decision aggregation point, which is the component responsible for privacy conflict detection and resolution

- **Policy conflict resolution** handles the set of all relevant rulings to solve conflicts and the generation of the final access control decision according to the selected strategy.

The functions described above run over a specified number of iterations, leading to a specific number of access requests, and so of privacy conflict detection and resolution. Some iterations are used for measurement (i.e., milestones) of the equity using the Gini coefficient as stated in previous section.

6.3 The Experimental Setup

Simulations have been performed to evaluate the efficiency of the enforcement of privacy policies in the equity-preserving algorithm, as described in chapter 5. Furthermore, the conflict resolution strategies (deny, allow and majority) described in section 5.1.4 are also implemented. The SNS simulations are performed in two different experiments. The first one is related to a fictitious SNS, the second one takes some elements from a real SNS. In both simulations, data differ in terms of number of users, number of interactions and distributed resources.

In an effort to facilitate the experimental validation of the current version of the equity algorithm, in this thesis the user's consent regarding disclosure of personal information is mechanically handled by the algorithm.

The adopted solution described above is not suitable in real SNS applications, in which consent should be explicitly obtained from users, according to regulations as pointed out in section 1.3.3. The users' consent should be obtained at the Policy Decision Point (PDP) level of the information sharing architecture proposed in section 5.1.2. On every access request, the Decision Aggregation Point (DAP) will interact with PDPs, ensuring that users explicitly express consent to the proposed processing of their personal information using either of the two strategies proposed in section 5.3. After DAP legitimates the request, it will send the access request decision to the Policy Enforcement Point (PEP).

6.3.1 Fictitious SNS Experiment

The fictitious SNS experiment is an artificial social network generated from a small graph of ten fictitious users, with a simulated behaviour regarding access control policies. In this experiment, users' PR are randomized. Four users are involved in each data access request. In order to validate whether the equity-preserving algorithm improves equity in the SNS, a drastically unbalanced population was artificially designed in which all interactions are in conflict. One user always answers "deny", and the other users always answer "allow" to user requests. The Gini coefficient is calculated on an average of 100 runs, using the normalized NPE (see Equation 6.2) in order to compute inequity based on the economic principle of income. Equation 6.1 is used to calculate the Gini coefficients for thirteen milestones in this experiment (after 20, 50, 100, 250, 500, 700, 1000, 1500, 2000, 3000, 3500 and 4000 interactions).

The experimental outcome is presented in Figure 6.4. In the "deny" strategy, a single user always wins (and increases her NPE), while others always lose. The result leads to a

very inequitable situation, and thus a very high Gini coefficient. The bad result of the "deny" strategy is not really surprising, since the population in this experiment is designed to obtain strong inequity, since just a person in the society always wins against everyone else. Indeed, the "deny" strategy reaches the upper bound of the Gini coefficient, which is $(n-1)/n$ [YS13].

In both "allow" and "majority" strategies, nine users always win (increasing their NPE) and one user always loses. These two strategies mechanically get significantly better results, and a pretty small (and constant) Gini coefficient.

Finally, the "equity" strategy proposed in this thesis achieves the best results in this population, because it ensures that everyone reaches the same enforcement rate, leading to a quick convergence towards 0 for the Gini coefficient. In this basic example at least, no other resolution strategy achieves a better result.

One should note that even though the difference between the Gini coefficients of the equity strategy and of the other "efficient" strategies (all but deny) is only about 0.1, it is still a significant result when it comes to Gini coefficients. As an example, one can find a similar difference between the Gini coefficients measuring the 2005 income inequities in Sweden (Gini 0.250) and Egypt (Gini 0.344) [GSS07].

Of course, this fictitious experiment and its sample size is not large enough to prove that the "equity" strategy reduces inequity properly, but the results confirm that the basic concepts of the equity-preserving algorithm are sound. However, more realistic experiments are now needed to evaluate the actual impact of the "equity" strategy.

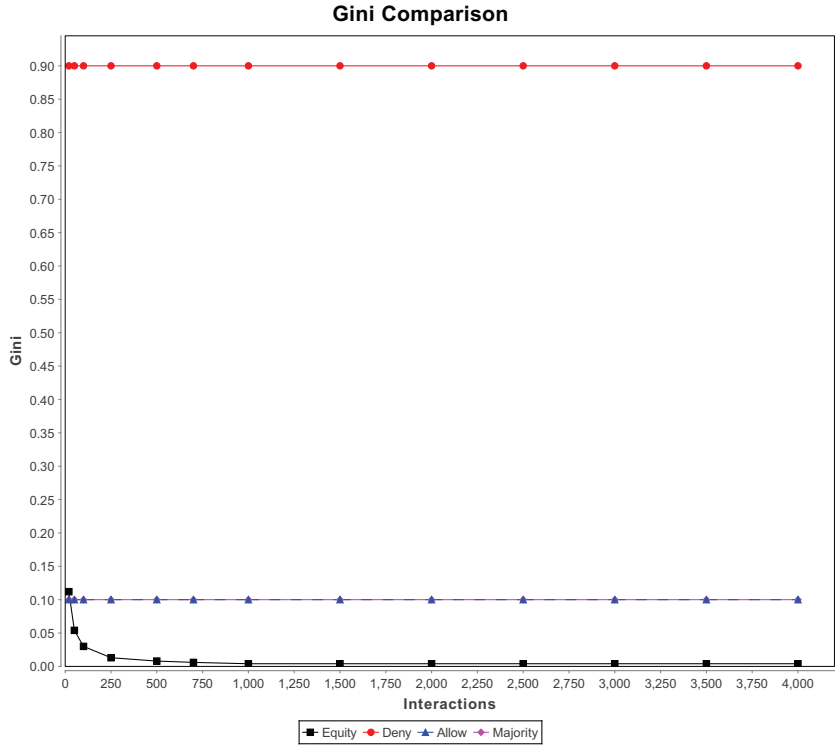

Figure 6.4 – Strategy results in a very unbalanced population

6.3.2 Facebook SNS Experiment

In order to simulate a more complex and realistic scenario, the first necessary step consists in obtaining a large, real-world network structure. For this purpose, a Facebook social graph comprising 4,039 users, obtained from the Stanford University database[1] was used. For each user, one or two resources (e.g., photos) have been randomly generated, and according to research works related to face recognition in online albums [DSC+05, NYGMP05], each resource is tagged and associated to two, three or four users, randomly chosen among friends and friends of friends. In this second experiment, users' PR are randomized. The Gini coefficient is calculated on an average of 100 runs, using the maximal inequity between normalized NPE and normalized NPV, as presented in Equation 6.2, in order to compute the worst inequity result. In this experiment, the worst result was reached by the normalized NPV for all strategy, which represents the rejection of a user's policy.

Equation 6.1 is used to calculate the Gini coefficients for seventy-eight milestone iterations (between 20 and 40.000 interactions). In the light of some studies showing that the majority of the users (75-80%) choose to approve tag requests [KLM+12, BRL10], the population for the experiment was designed considering that 20% of the users always answer "deny", while the rest of users always answer "allow" to a user request. Since not all interactions are in conflict, two situations need to be taken into account: if a conflict happens, NPV is incremented based on the chosen strategy, otherwise users' NPV are not incremented.

The experimental results are presented in Figure 6.5. One of the reasons for high inequity at the beginning of the interaction for all strategies is due to the computation of a Gini coefficient based on few interactions (e.g., 20, 50, 100 ...), where only a very small fraction of the users, in proportion to the population size, have interacted and updated their metrics.

In the "deny" strategy, at each interaction the majority of users have their policy rejected (which increases their NPV), while a few have their policy enforced. In consequence, the Gini coefficient decreases until 0.42 (a Gini coefficient between 0.4 and 0.5 usually indicates a large inequity[2]).

In both "allow" and "majority" strategies, at each interaction a few users have their policy rejected (which increases their NPV) while many users have their policy enforced. These two strategies lead to a very high inequity and thus a very high Gini coefficient of 0.79 for "allow" and 0.76 for "majority" (when the Gini coefficient reaches around 0.5, the inequity is considered extremely severe[3]). The Gini coefficient for "allow" and "majority" strategies are higher than for "deny" strategy, since the rate of inequity increases when a specific resource is concentrated by the minority of the population.

Finally, the considered proposal called "equity" strategy achieves the best results with a Gini coefficient of 0.21, since it ensures a relatively uniform distribution without much concentration of policy rejection in the population. The equity result is in accordance with values for countries with relative equitable distribution which usually range between 0.20 and 0.30, since in reality a theoretical perfect equity (Gini 0) is never observed [TS09]. One should note that, even though the difference between the Gini coefficients of the "equity"

[1] https://snap.stanford.edu/data/egonets-Facebook.html
[2] http://www.marketwatch.com/story/china-refuses-to-release-gini-coefficient-2012-01-18
[3] http://www.marketwatch.com/story/china-refuses-to-release-gini-coefficient-2012-01-18

strategy and "deny" strategy is only about 0.2, a similar difference was measured between the 2005's income inequities in Sweden (Gini 0.250) and in Iran (Gini 0.430) [GSS07]. In fact, this result can be considered a significant improvement when compared to classical conflict resolution algorithms.

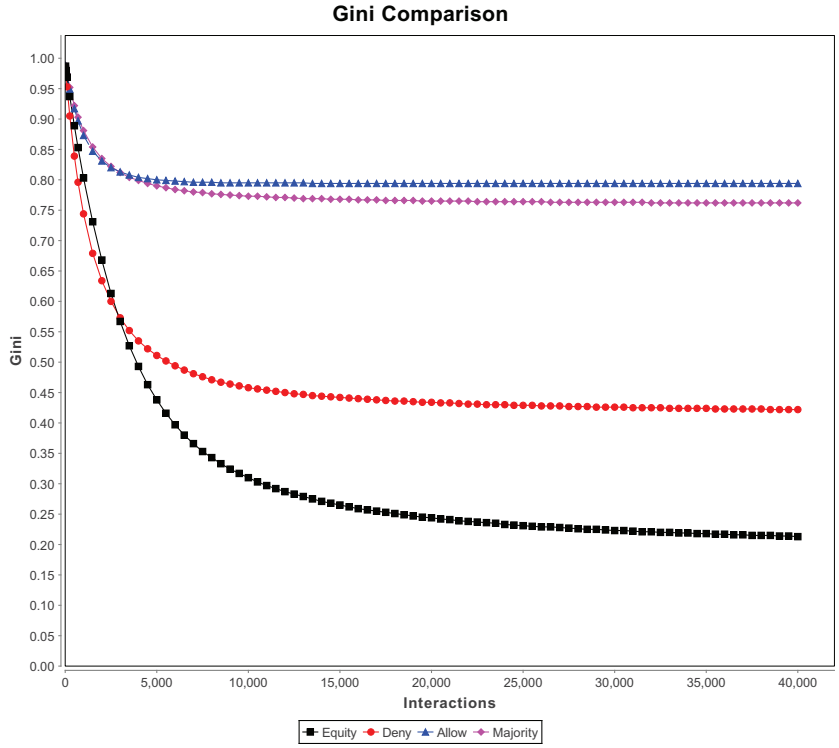

Figure 6.5 – The strategies' outcomes using the Facebook population

6.4 Discussion

6.4.1 Limitations of the Implementation

The current implementation of the equity-preserving conflict management algorithm considers only rulings of privacy policies that seems sufficient to validate the equity strategy. However, the prototype can be improved to generate more-complex rules without losing its ease of use. Indeed, each user's privacy policy is coarsely approximated through machine-generated rules. In order to get an idea of the true impact of the equity resolution strategy on the overall behaviour of a real SNS, additional user profiles rulings determining their responses to access requests can be more expressive, subtle and realistic.

A possible enhancement of the algorithm could be to decentralize it. The current implementation uses a single Decision Aggregation Point. It should be possible to perform the ruling aggregation of an access request at any node of the network, measuring equity in a

reliable way (users should not be able to fake their history metrics, corrupt the algorithm and manipulate the outcome rulings).

6.4.2 Impact of Design Choices

The degree of decentralization (centralized, decentralized or fully decentralized) of the privacy-related properties presented in section 4.2 might play a major role according to the chosen conflict resolution strategy.

On the one hand, the traditional "deny", "allow" and "majority" strategies do not need a history of past operations for a given access request. The required information for these strategies is an access request and the set of relevant individual rulings. Therefore, these traditional strategies easily allow a decentralized management of policies and conflicts because independent conflict situations can be handled by different DAPs. If the deny strategy is considered when there is an access request, the PDPs involved in the conflict send their relevant rulings to an appropriated DAP that locally verify in peers or super-peers (depending on the degree of decentralization) if any PDP has send a deny ruling, generating the final answer "deny".

On the other hand, however, the equity strategy requires to keep some history of past operations in the form of the NPV, NPE, and NI metrics in order to operate. The management of the history in the information sharing architecture proposed in section 5.1.2 must take into account the many distinct PDPs, each corresponding to a different user policy. However, this architecture identifies and resolves conflicts using a single DAP. Due to the autonomy of PDPs, peer policies administration may be handled in a distributed or fully distributed manner, while peer policy enforcement is more naturally centralized, due to the unique DAP.

Limiting the architecture to a single DAP has the advantage of simplifying its implementation. Nonetheless, the central authority is a potential privacy risk of direct manipulations of these metrics (NPV, NPE, and NI), because the DAP keeps the metrics of all users once involved in the equity algorithm. Distributing a component such as DAP hence constitutes a difficult task in such an architecture for three reasons. The first one is that users may choose to misreport their metrics in an attempt to affect the equity strategy result to their advantage. A possible solution for this first issue would be the introduction of non-interactive zero-knowledge proofs, in which the prover is able to convince the verifier of the truthfulness of a statement [BFM88]. The second reason is that distributed DAPs should maintain the confidentiality of the users' metrics. An alternative solution for the second reason could be the use of cryptographic-based solutions such as secure multiparty computation, as mentioned in section 1.5. The third reason is that distributed DAPs should not alter users' metrics, which remain an open issue that should be more profoundly studied.

In addition, the DAP also interacts with the PEP, a component responsible for enforcing privacy policies. The PEP enforces the access decision to the data storage space, and can be implemented in a decentralized or fully decentralized fashion. In a distributed architecture, peer policy enforcement involves many PEPs should be used for every storage space throughout the network. Therefore, storage space can also be decentralized or fully decentralized since the enforcement decision takes place where the location of the required data resides.

The proposed architecture in section 5.1.2 has distributed PDPs, but centralized DAP and PEP assuming a trusted environment without any additional protection of data. Having the referred architecture in a untrusted fashion, the data confidentiality can be guaranteed by using encryption. If the data is encrypted, then the PEP should be distributed in the sense that every storage data should have a local PEP to enforce the policy decisions. It other words, PEPs should be deployed to execute two different tasks: (1) to enforce the access decision that conveys from the DAP, and (2) to enforce the protection of stored data.

6.5 Conclusion

This chapter presented a proof-of-concept implementation of the equity-preserving algorithm and showed through experimentation that the equity strategy actually reduces existing inequities in terms of policy enforcement.

To evaluate the performance of the equity-preserving strategy, two simulations have been performed and results are compared to the deny, allow, and majority strategies by using the Gini coefficient to measure inequity. The originality of this work is the use of the Gini coefficient to measure inequities in the enforcement of privacy policies. The evaluation conducted shows that the equity-preserving approach leads to better results than classical conflict resolution strategies.

The experiments show two important topics to be considered:

- The fictitious SNS experiment allows to exemplify the extremal case of perfect inequity for "deny" strategy and perfect equity for "equity" strategy. These cases can be observed because all interactions are in conflict and responses are static. Moreover, since the population is a small graph with the limited number of ten users and less diversity in their profiles, the estimation of the upper bound of the Gini coefficient is affected. It means that the upper bound of the Gini coefficient should be one, but in practice is equal to $(n-1)/n$ [YS13]. This result is confirmed by the fictitious SNS experiment. A similar result was found in Cojocaru [Coj14], where for a small sample size the estimation of the Gini introduces a downward bias;

- The Facebook SNS experiment shows realistic results in accordance with values of the Gini coefficient for income distribution in countries. These values usually range between 0.20 and 0.30 for countries with relative equitable distributions and between 0.50 and 0.70 for countries with highly inequity income distributions [TS09].

Conclusions and future works

The last decade has seen the growth of Social Network Systems (SNSs). In their very beginnings SNSs started as niche applications, and nowadays with the increasing usage in a variety of new modes of interactions, they are widely accepted in the world. Besides having positive aspects, SNSs also present negative impacts on users' privacy. The large amount of available SNSs relies on centralized architectures that threaten users' privacy.

Privacy limitations posed by centralized SNSs have motivated the development of decentralized alternatives that work toward decentralizing the infrastructure support. Decentralized SNSs capture the multidimensional concept of privacy by focusing on the protection of users' personal data, allowing them to keep control over data upon collection, use, and dissemination. Censorship from the SNS provider can also be avoided. Based on the hypothesis that avoiding central authorities prevent users' privacy violations, this thesis has developed a multi-criteria analysis grid to analyze and compare SNSs. The analysis grid is built on the degrees of decentralization, which enables an accurate analysis to evaluate several properties of SNSs. Then, lattice theory was applied to this grid, allowing to build a comprehensive structure aimed at identifying which SNS performs better with respects to a given property, and more generally at comparing SNS platforms in terms of privacy protection. Using the proposed lattice structure, it is possible to classify, evaluate and visualize SNSs within a partial hierarchy based on lattice chains and levels.

Following the motivation of this thesis to improve the general level of privacy in SNSs, the concept of privacy policies can be used to preserve users' privacy from unauthorized data access from other users. These policies enable users to control the access to their shared information according to privacy settings. The information shared in such systems can be associated with multiple users, hence involving different privacy settings for each one. Managing different privacy policies specified by the data publisher and her relationships can lead to policy conflicts and unfair situations. Therefore, it is important to examine the issue of handling conflicting privacy policies in the context of SNSs.

In this thesis, a management mechanism and the development of an equity-preserving algorithm to tackle the issue of equitable enforcement of multiple users' policies in SNSs is proposed. This original contribution provides and integrates the concept of equity in the field of policy conflict management, and in particular in the context of privacy policies. The equity-preserving algorithm showed, through simulations based on experimentation and real data, that the equity strategy actually reduce existing inequities, leading to better results than classical conflict resolution strategies in terms of policy enforcement, with respect to

the Gini coefficient, which is a standard metric for inequity in economics.

Future works include enrichment of the multi-criteria analysis grid with properties specifically linked to the privacy policies themselves, especially in terms of expressivity. This is another dimension along which it would be interesting to compare SNSs. Another possible future improvement could be the development of software components dedicated to the achievement of a given level of decentralization for a set of given properties. Such modular and reusable software, linked to the analysis tools presented in this thesis, could also be placed in the *privacy by design* conceptional framework.

In chapter 5 of this thesis an intuitive notion of equity in the field of policy conflict management has been introduced, but the concept and algorithm must be refined. The equity algorithm can be modified to take into account the privacy rank during the equity evaluation and the compensation phase. Further progress in this algorithm could be the development of a practical and realistic user tagging behaviour to support more sophisticated and flexible privacy policies.

The conceptualization of privacy as a collective understanding of societal situation's boundaries should be addressed not only from a technical but also from an societal, legal, and philosophical context. In this perspective, the elaboration of more complex and realistic scenarios to test the current version of the algorithm would allow to generate access requests and ruling conflicts at a larger scale (e.g., in a multi-agent environment constructed from the actual topology of an existing SNS). Likewise, the enrichment of the algorithm should involve the notion of obligation and purpose (associated to a ruling), presenting state-of-the-art policy languages. Finally, procedures considering the mathematical formulations of equity could be also a useful alternative for improving the formalization of policy conflict management.

If all these future work suggestions are accomplished, the corresponding software component could be an interesting tool for applying the principles of *Privacy by Design*, as well as incorporating the important concept of equity to the new SNSs.

Appendix A

Publications and Research Activities

During this thesis, various interactions with the scientific community were established which includes publications and presentations. They are summarized next.

- International Conferences
  - R. Marin, G. Piolle, and C. Bidan. Equity-preserving management of privacy conflicts in social network systems. In *The Sixth ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)*, Cambridge, MA, USA, December 2014. ASE.
  - R. Marin, G. Piolle, and C. Bidan. An analysis grid for privacy-related properties of social network systems. In *The Fifth ASE/IEEE International Conference on Social Computing (SocialCom 2013)*, pages 520–525, Alexandria, VA, USA, September 2013. IEEE.
- National Workshop
  - R. Paiva Melo Marin, G. Piolle, and C. Bidan. Privacy policy requirements for distributed social network systems. In *3rd Atelier sur la Protection de la Vie Privée (APVP'12)*, Groix, Britany, France, Jun 2012.

Bibliography

[ABvdT10] Guillaume Aucher, Guido Boella, and Leendert W. N. van der Torre. Privacy policies with modal logic: the dynamic turn. In *The 10th international conference on deontic logic in computer science (DEON'10)*, volume 6181 of *Lecture Notes in Computer Science*, pages 196–213, Fiesole, Italy, July 2010. Springer Berlin Heidelberg.

[AD07] Christopher Alm and Michael Drouineaud. Analysis of existing policy languages. Technical report, ORKA Organizational Control Architecture, 2007.

[AER02] A.I. Anton, J.B. Earp, and A. Reese. Analyzing website privacy requirements using a privacy goal taxonomy. In *IEEE Joint International Conference on Requirements Engineering*, pages 23–31, 2002.

[AG06] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Privacy Enhancing Technologies*, volume 4258 of *Lecture Notes in Computer Science*, pages 36–58. Springer Berlin Heidelberg, 2006.

[AGH09] Esma Aïmeur, Sébastien Gambs, and Ai Ho. Upp: User privacy policy for social networking sites. In *The Fourth International Conference on Internet and Web Applications and Services, 2009. ICIW '09.*, pages 267–272, May 2009.

[AGH10] Esma Aïmeur, Sébastien Gambs, and Ai Ho. Towards a privacy-enhanced social networking site. In *International Conference on Availability, Reliability, and Security (ARES)*, pages 172–179. IEEE Computer Society, 2010.

[AGR13] P. Anthonysamy, P. Greenwood, and A. Rashid. Social networking privacy: Understanding the disconnect from policy to controls. *Computer*, 46(6):60–67, June 2013.

[AGR14] Pauline Anthonysamy, Phil Greenwood, and Awais Rashid. A method for analysing traceability between privacy policies and privacy controls of online social networks. In *Privacy Technologies and Policy*, volume 8319 of *Lecture Notes in Computer Science*, pages 187–202. Springer Berlin Heidelberg, 2014.

[AHA11] Burhanuddin M. A., Sami M. Halawani, and A. R. Ahmad. A costing analysis for decision making grid model in failure-based maintenance. In *Advances in Decision Sciences*, 2011.

[AHKS02] Paul Ashley, Satoshi Hada, Günter Karjoth, and Matthias Schunter. E-p3p privacy policies and privacy authorization. In *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, WPES '02, pages 103–109, New York, NY, USA, 2002. ACM.

[Als12] Brendan Van Alsenoy. Allocating responsibility among controllers, processors, and everything in between: the definition of actors and roles in directive 95/46/ec. *Computer Law & Security Review*, 28(1):25 – 43, 2012.

[ARG11] Pauline Anthonysamy, Awais Rashid, and Phil Greenwood. Do the privacy policies reflect the privacy controls on social networks? In *The Third IEEE International Conference on Social Computing (SocialCom) and the Third IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT)*, pages 1155–1158. IEEE, 2011.

[AS11] E. Aïmeur and D. Schonfeld. The ultimate invasion of privacy: Identity theft. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*, pages 24–31, July 2011.

[Ash04] Paul Ashley. Enforcement of a p3p privacy policy. In *AISM*, pages 11–26. School of Computer and Information Science, Edith Cowan University, Western Australia, 2004.

[Ass48] United Nations General Assembly. Universal declaration of human rights (udhr), december 1948.

[Atk70] Anthony B Atkinson. On the measurement of inequality. *Journal of Economic Theory*, 2(3):244 – 263, 1970.

[AvdBN03] Roberto Abraham, Sidney van den Bergh, and Preethi Nair. A new approach to galaxy morphology: I. analysis of the sloan digital sky survey early data release. *Astrophysical Journal*, 588:218–229, 2003.

[AW11] A. Ahmad and B. Whitworth. Distributed access control for social networks. In *The 7th International Conference on Information Assurance and Security (IAS'11)*, pages 68–73, Dec 2011.

[Bar64] Paul Baran. On distributed communications networks. In *RAND Corporation papers*, 1964.

[BB11] W.J. Baumol and A.S. Blinder. *Microeconomics: Principles and Policy*. Cengage Learning, 2011.

[BBC05] BBC. News corp in $580m internet buy, june 2005.

[BBC+09] Elisa Bertino, Carolyn Brodie, Seraphin B. Calo, Lorrie Faith Cranor, Clare-Marie Karat, John Karat, Ninghui Li, Dan Lin, Jorge Lobo, Qun Ni, Prathima Rao, and Xiping Wang. Analysis of privacy and security policies. *IBM Journal of Research and Development*, 53(2):3, 2009.

[BBJ13] Frederic Besson, Nataliia Bielova, and Thomas Jensen. Seccloud: Quantitative information flow analysis against web tracking, 2013. CominLabs Week.

[BBS+09] Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, and Daniel Starin. Persona: An online social network with user-defined privacy. *SIGCOMM Comput. Commun. Rev.*, 39(4):135–146, aug 2009.

[BC03] P. Braveman and S. Cruskin. Defining equity in health. *Journal Epidemiology Community Health*, 57(4):254–258, oct 2003.

[BD09] S. Buchegger and A. Datta. A case for p2p infrastructure for social networks - opportunities & challenges. In *Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on*, pages 161–168, Feb 2009.

[BDMN06] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. Privacy and contextual integrity: Framework and applications. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, SP '06, pages 184–198, Washington, DC, USA, 2006. IEEE Computer Society.

[BDS04] Michael Backes, Markus Duermuth, and Rainer Steinwandt. An algebra for composing enterprise privacy policies. In *Proceedings of The 9th European Symposium on Research in Computer Security (ESORICS)*, volume 3193 of *LNCS*, pages 33–52. Springer, September 2004.

[BE07] Danah M. Boyd and Nicole B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), October 2007.

[Ben00] Roland Benabou. Unequal societies: Income distribution and the social contract. *The American Economic Review*, 90(1):96–129, 2000.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 103–112, New York, NY, USA, 1988. ACM.

[BHBL09] Christian Bizer, Tom Heath, and Tim Berners-Lee. Linked data-the story so far. *International journal on semantic web and information systems*, 5(3):1–22, 2009.

[Bie13] N. Bielova. Survey on javascript security policies and their enforcement mechanisms in a web browser. *Special Issue on Automated Specification and Verification of Web Systems of Journal of Logic and Algebraic Programming*, 2013.

[BJ06] M. Barbaro and T. Z. Jr. A face is exposed for aol searcher no. 441779, 2006.

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

[BKS+09] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, Tuomas Sandholm, Janice Tsai, Lorrie Faith Cranor, and Paul Hankes Drielsma. The impact of expressiveness on the effectiveness of privacy mechanisms for location-sharing. In *Proceedings of The 5th Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA, 2009. ACM.

[BKW09] Filipe Beato, Markulf Kohlweiss, and Karel Wouters. Enforcing access control in social network sites. In *Proceedings of The 2nd Hot Topics in Privacy Enhancing Technologies (HotPETs 2009)*, September 2009.

[BL09] Petter Bae Brondtzaeg and Marika Lüders. privacy 2.0 personal and consumer protection in new media reality. Technical report, SINTEF, 2009.

[BL11] Geoffrey Barbier and Huan Liu. Data mining in social media. In *Social Network Data Analytics*, pages 327–352. Springer US, 2011.

[BMB10] Moritz Y. Becker, Alexander Malkis, and Laurent Bussard. S4p: A generic language for specifying privacy preferences and policies. Technical Report MSR-TR-2010-32, Microsoft Research., 2010.

[Boy04] Danah M. Boyd. Friendster and publicly articulated social networking. In *CHI '04 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '04, pages 1279–1282, New York, NY, USA, 2004. ACM.

[Boy10] Danah M. Boyd. Making sense of privacy and publicity, march 2010.

[BPS03] Michael Backes, Birgit Pfitzmann, and Matthias Schunter. A toolkit for managing enterprise privacy policies. In *Proceedings of The 8th European Symposium on Research in Computer Security (ESORICS)*, volume 2808 of *Lecture Notes in Computer Science*, pages 162–180. Springer Berlin Heidelberg, 2003.

[BRL10] Andrew Besmer and Heather Richter Lipford. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of The SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[Bro94] Malcolm C. Brown. Using gini-style indices to evaluate the spatial patterns of health practitioners: Theoretical considerations and an application based on alberta data. *Social Science and Medicine*, 38(9):1243–1256, 1994.

[BSBK09] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *Proceedings of the 18th International Conference on World Wide Web*, WWW '09, pages 551–560, New York, NY, USA, 2009. ACM.

[BSVD09] Sonja Buchegger, Doris Schiöberg, Le-Hung Vu, and Anwitaman Datta. Peerson: P2p social networking: early experiences and insights. In *Proceedings of The Second ACM EuroSys Workshop on Social Network Systems*, pages 46–52, New York, NY, USA, 2009. ACM.

[Cav10] Ann Cavoukian. Privacy by design: The seven foundational principles, may 2010.

[CCBS05] F. Cuppens, N. Cuppens-Boulahia, and T. Sans. Nomad: a security model with non atomic actions and deadlines. In *Computer Security Foundations, 2005. CSFW-18 2005. 18th IEEE Workshop*, pages 186–196, June 2005.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of The Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, New York, NY, USA, 1988. ACM.

[CCT07] AmirH. Chinaei, HamidR. Chinaei, and FrankWm. Tompa. A unified conflict resolution algorithm. In *Secure Data Management*, volume 4721 of *Lecture Notes in Computer Science*, pages 1–17. Springer Berlin Heidelberg, 2007.

[CFP09] Barbara Carminati, Elena Ferrari, and Andrea Perego. Enforcing access control in web-based social networks. *ACM Trans. Inf. Syst. Secur.*, 13(1):6:1–6:38, nov 2009.

[Cha90] Satya R. Chakravarty. The gini indices of inequality. In *Ethical Social Index Numbers*, pages 82–113. Springer Berlin Heidelberg, 1990.

[CKGS98] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *J. ACM*, 45(6):965–981, November 1998.

[Cla14] Jason W. Clark. *Profiling, Tracking, and Monetizing: An Analysis of Internet and Online Social Network Concerns*. PhD thesis, George Mason University, August 2014.

[CMS09] L. A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *Comm. Mag.*, 47(12):94–101, dec 2009.

[CMS10] Leucio Antonio Cutillo, Mark Manulis, and Thorsten Strufe. Security and privacy in online social networks. In Borko Furht, editor, *Handbook of Social Network Technologies and Applications*, pages 497–522. Springer US, 2010.

[Coj14] Alexandru Cojocaru. Fairness and inequality tolerance: Evidence from the life in transition survey. *Journal of Comparative Economics*, 42(3):590 – 608, 2014.

[Con02] World Wide Web Consortium. A p3p preference exchange language 1.0, April 2002.

[Con06] World Wide Web Consortium. Platform for privacy preferences (P3P 1.1), November 2006.

[Cow09] F.A Cowell. Measuring inequality. Technical report, 2009.

[CP12] Luiz Costa and Yves Poullet. Privacy and the regulation of 2012. *Computer Law & Security Review*, 28(3):254 – 262, 2012.

[CPS13] Yuan Cheng, Jaehong Park, and Ravi Sandhu. Preserving user privacy from third-party applications in online social networks. In *Proceedings of The 22nd International Conference on World Wide Web Companion*, WWW '13 Companion, pages 723–728. International World Wide Web Conferences Steering Committee, 2013.

[Cra03] Lorrie Faith Cranor. P3p: Making privacy policies more useful. *IEEE Security and Privacy*, 1(6):50–55, nov 2003.

[CSA96] CSA. Model code for the protection of personal information. CSA CAN/CSA-Q830-96, Canadian Standards Association, march 1996.

[Cul01] Anthony J Culyer. Equity - some theory and its policy implications. *Journal of Medical Ethics*, 27(4):275 – 283, 2001.

[Cup93] Frédéric Cuppens. A logical analysis of authorized and prohibited information flows. In *IEEE Symposium on Research in Security and Privacy*, pages 100–109, Oakland, California, USA, 1993. IEEE Computer Society Press.

[CV12] Lidia Ceriani and Paolo Verme. The origins of the gini index: extracts from variabilit e mutabilit (1912) by corrado gini. *The Journal of Economic Inequality*, 10(3):421–443, 2012.

[DAM06] Yves Deswarte and Carlos Aguilar Melchor. Current and future privacy enhancing technologies for the internet. *Annales Des Tlcommunications*, 61(3-4):399–417, 2006.

[DBV+10] Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, and Krzysztof Rzadca. Decentralized online social networks. In Borko Furht, editor, *Handbook of Social Network Technologies and Applications*, pages 349–378. Springer US, 2010.

[DCdVS06] Sabrina De Capitani di Vimercati and Pierangela Samarati. Privacy in the electronic society. In Aditya Bagchi and Vijayalakshmi Atluri, editors, *Information Systems Security*, volume 4332 of *Lecture Notes in Computer Science*, pages 1–21. Springer Berlin Heidelberg, 2006.

[Deb11] Bernhard Debatin. Ethics, privacy, and self-restraint in social networking. In Sabine Trepte and Leonard Reinecke, editors, *Privacy Online*, pages 47–60. Springer Berlin Heidelberg, 2011.

[Dia14] Diaspora. Diaspora statistics, june 2014.

[DJZ+09] Ying Ding, Elin K. Jacob, Zhixiong Zhang, Schubert Foo, Erjia Yan, Nicolas L. George, and Lijiang Guo. Perspectives on social tagging. *J. Am. Soc. Inf. Sci. Technol.*, 60(12):2388–2401, dec 2009.

[DP90] Brian A. Davey and Hilary A. Priestley. *Introduction to lattices and order*. Cambridge University Press, Cambridge, 1990.

[DSC+05] Marc Davis, Michael Smith, John Canny, Nathan Good, Simon King, and Rajkumar Janakiraman. Towards context-aware face recognition. In *Proceedings of The 13th Annual ACM International Conference on Multimedia*, MULTIMEDIA '05, pages 483–486, New York, NY, USA, 2005. ACM.

[Dwo06] Cynthia Dwork. Differential privacy. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming*, volume 4052 of *Lecture Notes in Computer Science*, pages 1–12. Springer Berlin Heidelberg, 2006.

[EB13] N. B. Ellison and D. Boyd. Sociality through social network sites. In *The Oxford Handbook of Internet Studies*, pages 151–172. Oxford University Press, 2013.

[EC15] Martin Enserink and Gilbert Chin. The end of privacy. *Science*, 347(6221):490–491, 2015.

[EG85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[Eng12] Eric Engle. The history of the general principle of proportionality: An overview. *Dartmouth Law Journal*, 10:1–11, 2012.

[Eng13] Eric Engle. The general principle of proportionality and aristotle. In Liesbeth Huppes-Cluysenaer and Nuno M.M.S. Coelho, editors, *Aristotle and The Philosophy of Law: Theory, Practice and Justice*, volume 23 of *Ius Gentium: Comparative Perspectives on Law and Justice*, pages 265–276. Springer Netherlands, 2013.

[ET10] Patrick Van Eecke and Maarten Truyens. Privacy and social networks. *Computer Law & Security Review*, 26(5):535 – 546, 2010.

[Fac07] Facebook. Facebook platform, 2007.

[Fac14] Facebook. Facebook data use policy, october 2014.

[FAZ09] Philip W. L. Fong, Mohd Anwar, and Zhen Zhao. A privacy preservation model for facebook-style social network systems. In *Proceedings of the 14th European Conference on Research in Computer Security*, ESORICS'09, pages 303–320, Berlin, Heidelberg, 2009. Springer-Verlag.

[FHB13] Simone Fischer-Hübner and Stefan Berthold. Chapter 43 - privacy-enhancing technologies1. In John R. Vacca, editor, *Computer and Information Security Handbook (Second Edition)*, pages 755 – 772. Morgan Kaufmann, Boston, second edition edition, 2013.

[Fon11] Philip W.L. Fong. Relationship-based access control: Protection model and policy language. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*, CODASPY '11, pages 191–202, New York, NY, USA, 2011. ACM.

[fra78] République française. Loi numéro 78-17 du 6 janvier 1978 relative *à* l'informatique, aux fichiers et aux libertés. In European Union, editor, *Journal Officiel de la République Française*, Janvier 1978.

[GA05] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of The 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, pages 169–178, New York, NY, USA, 2009. ACM.

[Gin12] Corrado Gini. *Variabilitá e mutabilitá*. Cuppini, C., Bologna, Italy, 1912.

[GKB12] B. Greschbach, G. Kreitz, and S. Buchegger. The devil is in the metadata - new privacy challenges in decentralised online social networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 333–339. IEEE, March 2012.

[GLYH11] Manish Gupta, Rui Li, Zhijun Yin, and Jiawei Han. An overview of social tagging and applications. In Charu C. Aggarwal, editor, *Social Network Data Analytics*, pages 447–497. Springer US, 2011.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *Proceedings of*

the Fourteenth Annual ACM Symposium on Theory of Computing, STOC '82, pages 365–377, New York, NY, USA, 1982. ACM.

[GMR85] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 291–304, New York, NY, USA, 1985. ACM.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, February 1989.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of The Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 218–229, New York, NY, USA, 1987. ACM.

[Gol07] Ian Goldberg. Privacy enhancing technologies for the internet iii: Ten years later. In *Digital Privacy: Theory, Technologies and Practices*, pages 3–18. Auerbach Publications, New York, London, 2007.

[Goo07] Google. Open social, 2007.

[GPET03] Daniel Gianola, Miguel Perez-Enciso, and Miguel A. Toro. On marker-assisted prediction of genetic value beyond the ridge. *Genetics*, 163(1):347–365, may 2003.

[GS12] Wajeb Gharibi and Maha Shaabi. Cyber threats in social networking websites. *International Journal of Distributed and Parallel Systems (IJDPS)*, 3(1), 2012.

[GSS07] Richard Grabowski, Sharmistha Self, and Michale P. Shields. *Economic Development: A Regional, Institutional, and Historical Approach*. M. E. Sharpe, 2007.

[GTF08] Saikat Guha, Kevin Tang, and Paul Francis. Noyb: Privacy in online social networks. In *Proceedings of the First Workshop on Online Social Networks*, WOSN '08, pages 49–54, New York, NY, USA, 2008. ACM.

[Gür10] Fahriye Seda Gürses. *Multilateral Privacy Requirements Analysis in Online Social Network Services*. PhD thesis, Katholieke Universiteit Leuven, May 2010.

[GZ09] Paolo Guarda and Nicola Zannone. Towards the development of privacy-aware systems. *Inf. Softw. Technol.*, 51(2):337–350, feb 2009.

[HAJ11] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of The 27th Annual Computer Security Applications Conference (ACSAC'11)*, pages 103–112, New York, NY, USA, 2011. ACM.

[Hay73] F. A. Hayek. *Law, Legislation and Liberty: Rules and Order v. 3: A New Statement of the Liberal Principles of Justice and Political Economy*. Routledge & Kegan Paul Books, 1973.

[HHA+14] Tomer Hasson, Irit Hadar, Oshrat Ayalon, Sofia Sherman, Eran Toch, and Michael Birnhack. Are designers ready for privacy by design? examining perceptions of privacy among information systems designers. In *The 42nd Research Conference on Communication, Information and Internet Policy*, March 2014.

[HKP12] Julia Heidemann, Mathias Klier, and Florian Probst. Online social networks: A survey of a global phenomenon. *Comput. Netw.*, 56(18):3866–3878, dec 2012.

[Ho12] Ai T. Ho. *Towards a Privacy-Enhanced Social Networking Site*. PhD thesis, Montreal University, 2012.

[Hol09] Jan Holvast. History of privacy. In *The Future of Identity in the Information Society*, volume 298 of *IFIP Advances in Information and Communication Technology*, pages 13–42. Springer Berlin Heidelberg, 2009.

[Hol12] Nielsen Holdings. State of the media: The social media report. Technical report, Nielsen Holdings, 2012.

[HT13] Mireille Hildebrandt and Laura Tielemans. Data protection by design and technology neutral law. *Computer Law & Security Review*, 29(5):509 – 521, 2013.

[ISO96] ISO. Information technology – open systems interconnection – security frameworks for open systems: Access control framework. ISO ISO/IEC 10181-3:1966, International Organization for Standardization, Geneva, Switzerland, 1996.

[ISO08] ISO. Common criteria for information technology security evaluation- part 2: Security functional components. ISO ISO/IEC 15408 Standard, International Organization for Standardization, Geneva, Switzerland, 2008.

[IW03] IBM Tivoli and World Wide Web Consortium. Enterprise privacy authorization language (EPAL 1.2), November 2003.

[JL00] WBP Raamwerk J.P. Leerentveld, G. W. van Blarkom. Wbp raamwerk privacy audit. Technical report, The Hague, 2000.

[JM98] Deborah G. Johnson and Keith Miller. Anonymity, pseudonymity, or inescapable identity on the net (abstract). In *Proceedings of the Ethics and Social Impact Component on Shaping Policy in the Information Age*, ACM POLICY '98, pages 37–38, New York, NY, USA, 1998. ACM.

[JSSB97] Sushil Jajodia, Pierangela Samarati, V. S. Subrahmanian, and Eliza Bertino. A unified framework for enforcing multiple access control policies. *SIGMOD Rec.*, 26(2):474–485, jun 1997.

[KA10] Lalana Kagal and Hal Abelson. Access control is an inadequate framework for privacy protection. 2010. accessible in 01/12/2011.

[Kar12] Komathy Karuppanan. Security, privacy, and trust in social networks. In Ajith Abraham, editor, *Computational Social Networks*, pages 23–53. Springer London, 2012.

[KBCR09] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A nutrition label for privacy. In *Proceedings of The 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 4:1–4:12, New York, NY, USA, 2009. ACM.

[Kea10] P. A. Keane. The 2009 wa lee lecture in equity: the conscience of equity. *Law and Justice Journal*, 10(1):106–131, 2010.

[KGC06] SebastianMarius Kirsch, Melanie Gnasa, and ArminB. Cremers. Beyond the web: Retrieval in social information spaces. In Mounia Lalmas, Andy MacFarlane, Stefan Rger, Anastasios Tombros, Theodora Tsikrika, and Alexei Yavlinsky, editors, *Advances in Information Retrieval*, volume 3936 of *Lecture Notes in Computer Science*, pages 84–95. Springer Berlin Heidelberg, 2006.

[KK07] Matia Karyda and Spyros Kokolakis. Privacy perceptions among members of online communities. In *Digital Privacy: Theory, Technologies, and Practices*, page 253266. Auerbach Publications, 2007.

[KLM+12] Peter Klemperer, Yuan Liang, Michelle Mazurek, Manya Sleeper, Blase Ur, Lujo Bauer, Lorrie Faith Cranor, Nitin Gupta, and Michael Reiter. Tag, you can see it!: Using tags for access control in photo sharing. In *Proceedings of The SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 377–386, New York, NY, USA, 2012. ACM.

[KSW03] Günter Karjoth, Matthias Schunter, and Michael Waidner. Platform for enterprise privacy practices: Privacy-enabled management of customer data. In *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, PET'02, pages 69–84, Berlin, Heidelberg, 2003. Springer-Verlag.

[KW09] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. In *Proceedings of The 2nd ACM Workshop on Online Social Networks*, WOSN '09, pages 7–12, New York, NY, USA, 2009. ACM.

[LCM13] Zhuoshu Li, Yu-Han Chang, and Rajiv Maheswaran. Graph formation effects on social welfare and inequality in a networked resource game. In ArielM. Greenberg, WilliamG. Kennedy, and Nathan D. Bos, editors, *Social Computing, Behavioral-Cultural Modeling and Prediction*, volume 7812 of *LNCS*, pages 221–230. Springer, 2013.

[Leg03] Decreto Legislativo. Codice in materia di protezione dei dati personali. In *Gazzetta Ufficiale*, june 2003.

[LHB+14] Timo Leimbach, Dara Hallinan, Daniel Bachlechner, Arnd Weber, Maggie Jaglo, Leonhard Hennen, Rasmus jvind Nielsen, Michael Nentwich, Stefan Strauss, Theo Lynn, and Graham Hunt. Potential and impacts of cloud computing services and social network websites. Technical Report QA-01-14-011-EN-C, European Parliamentary Research Service, Enschede, January 2014.

[LHDL04] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. *Personal Ubiquitous Comput.*, 8(6):440–454, nov 2004.

[Lik32] R. Likert. A technique for the measurement of attitudes. *Archives of Psychology*, 22(140):1–55, 1932.

[LPL+03] Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura, and Sumit Shah. First experiences using xacml for access control in distributed systems. In *Proceedings of the ACM Workshop on XML Security*, XMLSEC 2003, pages 25–37, New York, NY, USA, 2003. ACM.

[LRS98] F.A. Lootsma, R. Ramanathan, and H. Schuijt. Fairness and equity via concepts of multi-criteria decision analysis. In TheodorJ. Stewart and RobinC. van den Honert, editors, *Trends in Multicriteria Decision Making*, volume 465 of *Lecture Notes in Economics and Mathematical Systems*, pages 215–226. Springer Berlin Heidelberg, 1998.

[LT10] Kun Liu and Evimaria Terzi. A framework for computing the privacy scores of users in online social networks. *ACM Trans. Knowl. Discov. Data*, 5(1):6:1–6:30, dec 2010.

[MAYLL+09] Ching Man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, and Tim Berners-Lee. Decentralization: The future of online social networking. In *W3C Workshop on the Future of Social Networking Position Papers*, 2009.

[MESW01] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen. Policy core information model – version 1 specification, February 2001.

[Mét09] Daniel Le Métayer. A formal privacy management framework. In Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, editors, *Formal Aspects in Security and Trust*, volume 5491 of *Lecture Notes in Computer Science*, pages 162–176. Springer Berlin Heidelberg, 2009.

[Mil67] Stanley Milgram. The small world problem. *Psychology Today*, 2:60–67, 1967.

[MKGV07] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, 1(1), mar 2007.

[MM09] Daniel Le Métayer and Shara Monteleone. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law & Security Review*, 25(2):136 – 144, 2009.

[MPB13] R. Marin, G. Piolle, and C. Bidan. An analysis grid for privacy-related properties of social network systems. In *The Fifth ASE/IEEE International Conference on Social Computing (SocialCom 2013)*, pages 520–525, Alexandria, VA, USA, September 2013. IEEE.

[MPB14] R. Marin, G. Piolle, and C. Bidan. Equity-preserving management of privacy conflicts in social network systems. In *The Sixth ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)*, Cambridge, MA, USA, December 2014. ASE.

[MS11] D. Malandrino and V. Scarano. Supportive, comprehensive and improved privacy protection for web browsing. In *The Third IEEE International International Conference on Privacy, Security, Risk and Trust (PASSAT 2011)*, pages 1173–1176, Oct 2011.

[MS14] Thomas More and Edmund Spenser. *Equity in English Renaissance Literature*. Routledge, 2014.

[MSS13] D. Malandrino, V. Scarano, and R. Spinelli. How increased awareness can impact attitudes and behaviors toward online privacy protection. In *The Fifth International Conference on Social Computing (SocialCom 2013)*, pages 57–62, Sept 2013.

[Mül06] Günter Müller. Introduction of privacy and security in highly dynamic systems. *Communications of the ACM*, 49(9):1013–1022, 2006.

[Nar03] Enrico Nardelli. *Certification and Security in E-Services from E-Government to E-Business*. Kluwer, 2003.

[Nar12] Rammohan Narendula. The case of decentralized online social networks. Technical Report Infoscience, EPFL, 2012.

[Nas10] Robayet Nasim. Privacy-enhancing access control mechanism in distributed online social network. Master's thesis, Royal Institute of Technology, 2010.

[NBL08] Qun Ni, Elisa Bertino, and Jorge Lobo. An obligation model bridging access control policies and privacy policies. In *Proceedings of The 13th ACM Symposium on Access Control Models and Technologies*, SACMAT '08, pages 133–142, New York, NY, USA, 2008. ACM.

[NCM13] Bowen Ni, Yu-Han Chang, and Rajiv Maheswaran. Social welfare and inequality in a networked resource game with human players. *IEEE International Conference on Social Computing/IEEE International Conference on Privacy, Security, Risk and Trust*, pages 967–970, 2013.

[NIS09] NIST. Guide to protecting the confidentiality of personally identifiable information (pii). NIST Special Publication 800-122, National Institute of Standards and Technology, Jan 2009.

[NPA12] R. Narendula, T.G. Papaioannou, and K. Aberer. Towards the realization of decentralized online social networks: An empirical study. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, pages 155–162, June 2012.

[NS08] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 111–125, May 2008.

[NTB+12] Arvind Narayanan, Vincent Toubiana, Solon Barocas, Helen Nissenbaum, and Dan Boneh. A critical look at decentralized personal data architectures. *CoRR*, 2012.

[NYGMP05] Mor Naaman, Ron B. Yeh, Hector Garcia-Molina, and Andreas Paepcke. Leveraging context to resolve identity in photo albums. In *Proceedings of The 5th ACM/IEEE-CS Joint Conference on Digital Libraries*, JCDL '05, pages 178–187, New York, NY, USA, 2005. ACM.

[OEC80] OECD. Guidelines on the protection of privacy and transborder flows of personal data. Technical report, OECD, September 1980.

[OEC13] OECD. The oecd privacy framework. Technical Report C(2013)79, OECD, July 2013.

[Org14] Organization for the Advancement of Structured Information Standards. extensible access control markup language, march 2014.

[Ort96] Rodolphe Ortalo. Using deontic logic for security policy specification. LAAS report 96380, LAAS-CNRS, Toulouse, France, october 1996.

[otDPC98] Office of the Data Protection Commissioner. Data protection act. October 1998.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'99, pages 223–238, Berlin, Heidelberg, 1999. Springer-Verlag.

[PB13] Pallavi I. Powale and Ganesh D. Bhutkar. Overview of privacy in social networking sites (sns). *International Journal of Computer Applications*, 74(19):39–46, July 2013.

[PBS11] Thomas Paul, Sonja Buchegger, and Thorsten Strufe. Decentralizing social networking services. In Luca Salgarelli, Giuseppe Bianchi, and Nicola Blefari-Melazzi, editors, *Trustworthy Internet*, pages 187–199. Springer Milan, 2011.

[PCG03] D. Poo, B. Chng, and Jie-Mein Goh. A hybrid approach for user profiling. In *Proceedings of The 36th Annual Hawaii International Conference on System Sciences*, pages 9 pp.–, Jan 2003.

[PD10] Guillaume Piolle and Yves Demazeau. Déléguer la protection des données personnelles des agents cognitifs. *Revue d'Intelligence Artificielle*, 24(3/2010):357–390, June 2010.

[Pet02] Sandra Petronio. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press, Albany, New York, United States, 2002.

[PFS14] Thomas Paul, Antonino Famulari, and Thorsten Strufe. A survey on decentralized online social networks. *Computer Networks*, 75, Part A(0):437 – 452, 2014.

[PGW+08] J. A. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. H. J. Epema, M. Reinders, M. R. van Steen, and H. J. Sips. Tribler: A social-based peer-to-peer system: Research articles. *Concurr. Comput. : Pract. Exper.*, 20(2):127–138, February 2008.

[PMMPB12] R. Paiva Melo Marin, G. Piolle, and C. Bidan. Privacy policy requirements for distributed social network systems. In *3rd Atelier sur la Protection de la Vie Privée (APVP'12)*, Groix, Britany, France, Jun 2012.

[Pra14] Vaughan Pratt. Lattice theory, 2014. CS 353: Algebraic Logic.

[Pri67] Arthur Norman Prior. *Past, present and future*. Oxford University Press, 1967.

[PS14] Raúl Pardo and Gerardo Schneider. A formal privacy policy framework for social networks. In Dimitra Giannakopoulou and Gwen Salaün, editors, *Software Engineering and Formal Methods*, volume 8702 of *Lecture Notes in Computer Science*, pages 378–392. Springer International Publishing, 2014.

[PSS+07] Andreas Pfitzmann, Anne-Katrin Stange, Sandra Steinbrecher, Stefan Kopsell, and Andreas Juschka. Communication privacy. In *Digital Privacy: Theory, Technologies and Practices*, pages 19–46. Auerbach Publications, New York, London, 2007.

[PtC95] The European Parliament and the Council. Directive 1995/46/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. In European Union, editor, *Official Journal of the European Communities*, October 1995.

[PtC02] The European Parliament and the Council. Working document on determining the international application of eu data protection law to personal data processing on the internet by non-eu based websites. In European Union, editor, *Official Journal of the European Communities*, May 2002.

[PtC09] The European Parliament and the Council. Article 29 data protection working party, opinion 5/2009 on social network sites. In European Union, editor, *Official Journal of the European Communities*, Jun 2009.

[PtC13a] The European Parliament and the Council. Article 29 data protection working party, advice paper on essential elements of a definition and provision on profiling within the eu general data protection regulation. In European Union, editor, *Official Journal of the European Communities*, May 2013.

[PtC13b] The European Parliament and the Council. Article 29 data protection working party, advice paper on the police and criminal justice data protection directive. In European Union, editor, *Official Journal of the European Communities*, February 2013.

[PtC13c] The European Parliament and the Council. Draft version-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). In European Union, editor, *Official Journal of the European Communities*, October 2013.

[PZYD11] George Pallis, Demetrios Zeinalipour-Yazti, and Dikaiakos Marios D. Online social networks: Status and trends. In Athena Vakali and LakhmiC. Jain, editors, *New Directions in Web Data Management 1*, volume 331 of *Studies in Computational Intelligence*, pages 213–234. Springer Berlin Heidelberg, 2011.

[QCQ+12] Zheng Qin, Fei Chen, QiangWang, Alex X. Liu, and Zhiguang Qin. Towards high performance security policy evaluation. *Springer*, 59:1577–1595, June 2012.

[Raw71] John Rawls. *A Theory of Justice*. Atheneum, Harvard University Press, 1971.

[Rey03] Mark Reynolds. The complexity of the temporal logic with until over general linear time. *Journal of Computer and System Sciences*, 66(2):393–426, March 2003.

[RSS14] Ashwini Rao, Florian Schaub, and Norman Sadeh. What do they know about me? contents and concerns of online behavioral profiles. In *The Sixth ASE International Conference on Privacy, Security, Risk and Trust (PASSAT 2014)*, Cambridge, MA, USA, December 2014. ASE.

[RSV14] Emanuela Raffinetti, Elena Siletti, and Achille Vernizzi. On the gini coefficient normalization when attributes with negative values are considered. *Statistical Methods & Applications*, pages 1–15, 2014.

[SB04] Victor Sadras and Rodolfo Bongiovanni. Use of lorenz curves and gini coefficients to assess yield inequality within paddocks. *Field Crops Research*, 90(23):303–310, 2004.

[SC09] Sarah Spiekermann and Lorrie Faith Cranor. Engineering privacy. *IEEE Trans. Softw. Eng.*, 35(1):67–82, January 2009.

[Sch08] Doris Schiöberg. *A Peer-to-peer Infrastructure for Social Networks*. PhD thesis, TU Berlin, 2008.

[Sch11] Bart W. Schermer. The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1):45 – 52, 2011.

[SD12] Rajesh Sharma and Anwitaman Datta. Supernova: Super-peers based architecture for decentralized online social networks. In *Fourth International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–10. IEEE, 2012.

[SHC+09] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Comput.*, 13(6):401–412, August 2009.

[Shi94] Roger A. Shiner. Aristotle's theory of equity. *Loyola of Los Angeles Law Review*, 27(1245), 1994.

[SJB11] John W. Satzinger, Robert B. Jackson, and Stephen D. Burd. *Systems Analysis and Design in a Changing World*. Course Technology Press, Boston, MA, United States, 6th edition, 2011.

[SMK11] Rashid Sheikh, Durgesh Kumar Mishra, and Beerendra Kumar. Secure multiparty computation: From millionaires problem to anonymizer. *Inf. Sec. J.: A Global Perspective*, 20(1):25–33, January 2011.

[Sol03] Daniel J Solove. Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal*, 54:1227, 2003.

[Sol06] Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477–560, 2006.

[Sol12] Daniel J. Solove. Conceptualizing privacy. *California Law Review*, 90:1087, 2012.

[SS11] Paul M. Schwartz and Daniel J. Solove. The pii problem: Privacy and a new concept of personally identifiable information. *Communications of the ACM*, 86:1814, 2011.

[SSP09] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. Collective privacy management in social networks. In *Proceedings of The 18th International Conference on World Wide Web (WWW'09)*, pages 521–530, New York, NY, USA, 2009. ACM.

[SV10] N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography*, PKC'10, pages 420–443, Berlin, Heidelberg, 2010. Springer-Verlag.

[SVCC09] Amre Shakimov, Alexander Varshavsky, Landon P. Cox, and Ramón Cáceres. Privacy, cost, and availability tradeoffs in decentralized osns. In *Proceedings ofTthe 2nd ACM Workshop on Online Social Networks*, WOSN 2009, pages 13–18, New York, NY, USA, 2009. ACM.

[Swe97] Latanya Sweeney. Weaving technology and policy together to maintain confidentiality. *The Journal of Law, Medicine & Ethics*, 25(2-3):98–110, 1997.

[Swe02] Latanya Sweeney. K-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, October 2002.

[TC12] Antonio Tapiador and Diego Carrera. A survey on social network sites' functional features. *Computing Research Repository (CoRR)*, abs/1209.3650, 2012.

[The67] H. Theil. *Economics and Information Theory*. North-Holland, 1967.

[THZZ14] Yi Tao, Kizito Henry, Qinpei Zou, and Xiaoni Zhong. Methods for measuring horizontal equity in health resource allocation: a comparative study. *Health Economics Review*, 4(10), 2014.

[TKF11] F. Tegeler, D. Koll, and Xiaoming Fu. Gemstone: Empowering decentralized social networking with high data availability. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–6, Dec 2011.

[Tra12] DucA. Tran. Introduction. In *Data Storage for Social Networks*, SpringerBriefs in Optimization, pages 1–12. Springer New York, 2012.

[TS09] Michel Todaro and Stephen C. Smith. *Economics Development*. Pearson Addison Wesley, 2009.

[TSGW09] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, and Alec Wolman. Lockr: Better privacy for social networks. In *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, CoNEXT 2009, pages 169–180, New York, NY, USA, 2009. ACM.

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer Berlin Heidelberg, 2010.

[von51] Georg Henrik von Wright. Deontic logic. *Mind*, 60:1–15, 1951.

[WB90] Samuel D. Warren and Louis D. Brandeis. The right to privacy. *Harvard Law Review*, 4:193–195, 1890.

[Wes67] Alan F. Westin. *Privacy and freedom*. Atheneum, New York, 1967.

[WJ07] X. Sean Wang and Sushil Jajodia. Privacy protection with uncertainty and indistinguishability. In *Digital Privacy: Theory, Technologies, and Practices*, pages 173 –185. Auerbach Publications, 2007.

[WN13] Yong Wang and R.K. Nepali. Privacy measurement for social network actor model. In *The Fifth International Conference on Social Computing (SocialCom 2013)*, pages 659–664, Sept 2013.

[WS84] Jacob Weiner and Otto T. Solbrig. The meaning and measurement of size hierarchies in plant populations. *Oecologia*, 61(3):334–336, 1984.

[WZ11] Craig E. Wills and Mihajlo Zeljkovic. A personalized approach to web privacy - awareness, attitudes and actions. *Inf. Manag. Comput. Security*, 19(1):53–73, 2011.

[WZS+12] Xiao-jun Wang, Jian-yun Zhang, Shamsuddin Shahid, Amgad ElMahdi, Ruimin He, Xin-gong Wang, and Mahtab Ali. Gini coefficient to assess equity in domestic water supply in the yellow river. *Mitigation and Adaptation Strategies for Global Change*, 17(1):65–75, 2012.

[XV09] Xiao Xiao and Chris Varenhorst. Stop the tweet show: preventing harm and embarrassment to twitter user, april 2009.

[YK05] George Yee and Larry Korba. Specifying personal privacy policies to avoid unexpected outcomes. In *Proceedings of The Third Annual Conference on Privacy, Security and Trust (PST)*, 2005.

[YKP12] Akira Yamada, Tiffany Hyun-Jin Kim, and Adrian Perrig. Exploiting privacy policy conflicts in online social networks. Technical Report CMU-CyLab-12-005, Carnegie Mellon University, 2012.

[YPG00] R. Yavatkar, D. Pendarakis, and R. Guerin. A framework for policy-based admission control. Technical Report IETF, RCF 2753, United States, January 2000.

[YS13] Shlomo Yitzhaki and Edna Schechtman. More than a dozen alternative ways of spelling gini. In *The Gini Methodology*, volume 272 of *Springer Series in Statistics*, pages 11–31. Springer New York, 2013.

[ZG11] Elena Zheleva and Lise Getoor. Privacy in social networks: A survey. In *Social Network Data Analytics*, pages 277–306. Springer US, 2011.

[ZSZF10] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. Privacy and security for online social networks: challenges and opportunities. *Network, IEEE*, 24(4):13–18, July 2010.

Abstract

In Social Network Systems (SNSs), the sharing of information leads to many privacy concerns about potential abuses of personal information. Users' control over information shared with the SNS provider and with other users could be improved in SNSs through the decentralization of personal data, and the proper management of policy conflicts. Inspired by the decentralization approach, the first contribution of this thesis is the proposal of SNS design properties relevant to privacy when considered along a gradation of decentralization. These properties are organized in a multi-criteria analysis grid, designed to analyze and compare SNSs. The application of a lattice structure on this grid allows to evaluate, classify and visualize different SNSs within a partial hierarchy. While decentralization solves issues involving the SNS provider, privacy policies play a leading role in the protection of unauthorized data access from other users. The second contribution of this thesis consists in the introduction of the concept of equity in the context of policy conflict management. An algorithm to maintain equity between users in SNSs is introduced to solve conflicts that may arise between the privacy policies of several users, avoiding that some users take advantage over others. The evaluation shows that the equity approach introduced in this thesis leads to better results than classical conflict resolution strategies, reducing existing inequities in terms of policy enforcement.

Résumé

Le partage d'informations dans les systèmes de réseaux sociaux (SRS) suscite des inquiétudes concernant de possibles abus impactant la vie privée. La possibilité pour les utilisateurs de contrôler les informations qu'ils partagent avec le fournisseur de SRS et avec les autres utilisateurs peut être améliorée par la décentralisation des données personnelles et par une gestion appropriée des conflits entre politiques. Prenant son inspiration dans l'approche de décentralisation, la première contribution de cette thèse est la proposition de propriétés relevant de la conception du SRS et impactant la vie privée lorsqu'elles sont considérées par rapport à une gradation de la décentralisation. Ces propriétés ont été organisées dans une grille d'analyse multi-critères conçue pour analyser et comparer les SRS. L'application de la théorie des treillis à cette grille permet d'évaluer, de classifier et de visualiser différents SRS dans une hiérarchie partielle. Alors que la décentralisation résoud des problèmes impliquant le fournisseur de SRS, les politiques de vie privée jouent un rôle majeur dans la protection contre les accès non autorisés par d'autres utilisateurs. La seconde contribution de cette thèse consiste en l'introduction du concept d'équité dans le contexte de la gestion des conflits entre politiques. Un algorithme conçu pour maintenir l'équité entre les utilisateurs de SRS est introduit pour résoudre les conflits pouvant survenir entre les politiques de plusieurs utilisateurs, évitant que certains puissent gagner un avantage sur d'autres. L'évaluation montre que l'approche introduite dans cette thèse conduit à de meilleurs résultats que les stratégies classiques de résolution de conflits, réduisant ainsi les inéquités existantes en termes d'application des politiques.