Towards Assessing Information Privacy in Microblogging Online Social Networks.

THE IPAM FRAMEWORK

by SAMIA OUKEMENI

Universitat Oberta de Catalunya

Advisors: Dr. Helena Rifà-Pous & Dr. Joan Manuel Marquès Puig

PhD THESIS IN NETWORKS & INFORMATION TECHNOLOGIES

DOCTORAL THESIS

Towards Assessing Information Privacy in Microblogging Online Social Networks. The IPAM Framework

Author:
Samia OUKEMENI

Advisors:
Dr. Helena RIFÀ-POUS
Dr. Joan Manuel MARQUÈS PUIG

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

Doctoral Program in Networks and Information Technologies

K-ISON & ICSO

2016-2019

"East, West, South or North makes little difference. No matter what your destination, just be sure to make every journey, a journey within. If you travel within, you'll travel the whole wide world and beyond."

Elif Shafak

To my dear parents Hafida and Driss
For their unconditional love and endless encouragement

Abstract

Online Social Networks (OSNs) incorporate different forms of interactive communication, including microblogging services, multimedia sharing, business networking, etc. They allow users to create profiles, connect with friends, and share their daily activities and thoughts. The popularity of OSNs is due to the openness and the flexibility provided to the users. They can connect and communicate with their favorite celebrity, brand, politician, athlete or even other regular users without the obligation of a pre-existing social relationship.

The rapid expansion of OSNs, coupled with the increasing power of machine learning and data mining, have created new privacy concerns. By participating in OSNs, the users, voluntarily, share personal information about themselves and sometimes even sensitive information without prior knowledge of who can access their private data or how they are handled by the system. The data rich of personal information shared in the users' profiles or correlated from their activities can be stored, processed, analyzed, and sometimes sold for advertisement or statistical purposes. It attracts also malicious users who can collect and exploit the data and target different types of attacks. A chain of privacy-related public scandals linked to questionable data handling practices in OSNs has started to increase in the last past years. Thus, an effective and efficient evaluation of the privacy level provided in such services is necessary to meet user expectations and comply with the requirement of the applicable laws and regulations.

In the present thesis, we take first steps towards developing an information privacy assessment framework (IPAM framework) to compute privacy scores in Online Social Networks, and more specifically microblogging OSNs. The aim of the proposed framework is to help users identify risks related to their data and how their privacy is protected when using an OSN compared to others. The IPAM framework allows also comparing the privacy protection level between different systems, so that system providers can have an idea how they are positioned in the market vis-à-vis their competition and they can implement the recommendations provided to enhance their services.

This thesis improves the state-of-the-art in privacy evaluation and scoring in OSNs in several areas. In particular, the thesis contributes to the following aspects:

1. Analyzing the attitude of users towards their privacy in OSNs, and the factors that influence the sharing behavior.

2. Analyzing the state of the art and comparing 24 OSNs existing either in the literature or deployed for use. The analysis of each system is based on 7 criteria of comparison.

3. Presenting a generic framework to (1) guide the development of privacy metrics and (2) to measure and assess the privacy level of OSNs, more specifically microblogging systems. The algorithmic model is based on the impact of privacy and security requirements, accessibility, and difficulty of information extraction.

4. Finally, evaluating IPAM framework by comparing the surveyed social network systems with regards to their obtained privacy scores using the proposed algorithmic model.

Resumen

Las redes sociales on-line incorporan diferentes formas de comunicación interactiva como servicios de microblogueo, compartición de ficheros multimedia, o redes de contactos profesionales. Permiten a los usuarios crear perfiles, conectarse con sus amigos, y compartir sus actividades y pensamientos diarios. La popularidad de estas redes se debe a su flexibilidad de uso, ya que los usuarios pueden conectarse y comunicarse con sus famosos favoritos, marcas preferidas, políticos, u otros usuarios sin conocerse.

La rápida expansión de las redes sociales on-line, junto con el aprendizaje automático y la minería de datos, han creado nuevas amenazas de privacidad. Los usuarios, de manera voluntaria, comparten información personal e incluso a veces confidencial, sin conocer quién puede acceder a ella. Esta información puede ser procesada, analizada y, a veces vendida, a terceras empresas con fines publicitarios o estadísticos. En los últimos años han aumentado los escándalos públicos en relación con prácticas cuestionables de la industria de las redes sociales en relación a la privacidad. Así pues, es necesaria una evaluación efectiva y eficiente del nivel de privacidad en las redes sociales on-line para cumplir con las expectativas del usuario y cumplir con los requisitos de las leyes y regulaciones.

El foco de la presente tesis es la construcción de un esquema (IPAM) para identificar y evaluar el nivel de privacidad proporcionado por las redes sociales on-line, en particular para los servicios de microblogueo. El objetivo de IPAM es ayudar a los usuarios a identificar los riesgos relacionados con sus datos. El esquema también permite comparar el nivel de protección de la privacidad entre diferentes sistemas analizados, de modo que pueda ser también utilizado por proveedores de servicio y desarrolladores para probar y evaluar sus sistemas y si las técnicas de privacidad usadas son eficaces y suficientes.

Esta tesis mejora el estado del arte en la evaluación de la privacidad en sistemas de microblogueo. En particular, la tesis contribuye en los siguientes aspectos:

- Analizar la actitud de los usuarios en relación a la privacidad en redes sociales on-line, y los factores que influyen en el comportamiento de compartir informaciones personales.

- Analizar un estudio de revisión de 24 redes sociales on-line existentes en la literatura o implementadas para usar. El análisis de cada sistema se basa en 7 criterios de comparación.

- Presentar un esquema para (1) dirigir el desarrollo de métricas de privacidad y (2) evaluar el nivel de privacidad de las redes sociales on-line, más específicamente de los sistemas de microblogueo. El modelo algorítmico usado se basa en el impacto de los requisitos de privacidad y seguridad, la accesibilidad, y la dificultad de extracción de información.

- Finalmente, evaluar el esquema y comparar los sistemas de redes sociales online analizadas previamente con respecto a sus valores de privacidad obtenidos con el modelo propuesto.

Resum

Les xarxes socials online incorporen diferents formes de comunicació interactiva com a serveis de microblogs, compartició de fitxers multimèdia, o xarxes de contactes professionals. Permeten als usuaris crear perfils, connectar amb els seus amics, i compartir les seves activitats i pensaments diaris. La popularitat d'aquestes xarxes es deu a la seva flexibilitat d'ús, ja que els usuaris poden connectar-se i comunicar-se amb els seus famosos favorits, marques preferides, polítics, o altres usuaris sense conèixer-se.

La ràpida expansió de les xarxes socials en línia, juntament amb l'aprenentatge automàtic i la mineria de dades, han creat noves amenaces de privacitat. Els usuaris, de manera voluntària, comparteixen informació personal i fins i tot de vegades confidencial, sense conèixer qui pot accedir-hi. Aquesta informació pot ser processada, analitzada i, de vegades venuda, a terceres empreses amb finalitats publicitàries o estadístiques. En els últims anys han augmentat els escàndols públics en relació amb pràctiques qüestionables de la indústria de les xarxes socials en relació a la privacitat. Així doncs, cal una avaluació efectiva i eficient del nivell de privacitat en les xarxes socials on-line per complir amb les expectatives de l'usuari i complir amb els requisits de les lleis i regulacions.

El focus de la present tesi és la construcció d'un esquema (IPAM) per identificar i avaluar el nivell de privacitat proporcionat per les xarxes socials on-line, en particular per als serveis de microblogs. L'objectiu d'IPAM és ajudar els usuaris a identificar els riscos relacionats amb les seves dades. L'esquema també permet comparar el nivell de protecció de la privacitat entre diferents sistemes analitzats, de manera que pugui ser també utilitzat per proveïdors de servei i desenvolupadors per provar i avaluar els seus sistemes i si les tècniques de privacitat usades són eficaços i suficients.

Aquesta tesi millora l'estat de l'art en l'avaluació de la privacitat en sistemes de microblogs. En particular, la tesi contribueix en els següents aspectes:

- Analitzar l'actitud dels usuaris en relació a la privacitat en xarxes socials online, i els factors que influeixen en el comportament de compartir informacions personals.
- Analitzar un estudi de revisió de 24 xarxes socials on-line existents a la literatura o implementades per utilitzar. L'anàlisi de cada sistema es basa en 7 criteris de comparació.
- Presentar un esquema per a (1) dirigir el desenvolupament de mètriques de privacitat i (2) avaluar el nivell de privacitat de les xarxes socials en línia, més específicament dels sistemes de microblogs. El model algorítmic usat es basa en l'impacte dels requisits de privacitat i seguretat, l'accessibilitat, i la dificultat d'extracció d'informació.
- Finalment, avaluar l'esquema i comparar els sistemes de xarxes socials online analitzades prèviament respecte als seus valors de privacitat obtinguts amb el model proposat.

List of Publications

- ***Journals:***
  - **P1** Samia Oukemeni, Helena Rifà-Pous, and Joan Manuel Marquès Puig. 2019. "Privacy Analysis on Microblogging Online Social Networks: A Survey". In: ACM Comput. Surv. 52, 3, Article 60 (June 2019), 36 pages. DOI: https://doi.org/10.1145/3321481.
    JCR Impact Factor: 6.131 (2018), 1st quartile.
  - **P2** Samia Oukemeni, Helena Rifà-Pous, Joan Manuel Marquès Puig, and Jesica Pérez Guijarro. "Revisiting Privacy: Do We Really Care About Our Privacy in Online Social Networks?" (*under review, journal "Behaviour & Information Technology; JCR:1.429 (2018), 2nd quartile*).
  - **P3** Samia Oukemeni, Helena Rifà-Pous, and Joan Manuel Marquès Puig. "IPAM: Information Privacy Assessment Metric in Microblogging Online Social Networks". In IEEE Access, vol. 7, pp. 114817-114836, 2019. DOI: https://10.1109/ACCESS.2019.2932899.
    JCR Impact Factor: 4.098 (2018), 1st quartile.
- ***Workshops:***
  - **P4** Samia Oukemeni, Helena Rifà-Pous, and Joan Manuel Marquès Puig. "Privacy in Microblogging Online Social Networks: Issues and Metrics". In: Actas de la XV Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2018). Universidad de Garanada. 2018, pp. 107–112.

Acknowledgements

During my 3 years at the Universitat Oberta de Catalunya (UOC), I have had the opportunity of working with great colleagues that turned my doctoral experience into one I will cherish forever. First, I would like to express my endless gratitude and deep appreciation to my supervisors Dr. Helena Rifà-Pous and Dr. Joan Manuel Marquès Puig. I certainly would not have reached this far without your help, support, guidance, time, and patience during these past 3 years. Thank you very much!

Special thanks go to my dear friends Ronak, Leila, and Waseem. We came from different countries and cultures, but during these past 3 years, we have become one family. I am grateful that you are in my life. A big thank you to all my friends and colleagues from the doctoral school (students and staff), with whom I have spent endless hours discussing work and non-work related topics.

My sincere thanks to all the people who contributed in some way to the work described in this thesis. Special thanks go to the funding provided by the Ministry of Economy and Competitiveness in part under Grant RTI2018-095094-B-C22 "CONSENT", and in part under Grant TIN2014-57364-C2-2-R "SMARTGLACIS.

At last but not the least, I would like to extend my deepest gratitude to my family and friends. To my beloved parents, Hafida and Driss, I can't express enough my love to you. Thank you for your support, your encouragement, and for believing in me. I am so lucky to have parents like you. To my siblings, Mohammed Amine and Sofia, my sister-in-law Ihsane and my nephew Iyad, thank you for your love and continuous encouragement. I would like also to thank my dear friend Claudia for everything you have done for me and for putting up with me during these years. My thanks extend also to all my friends, you have made my journey in Barcelona very enjoyable.

To all members of my family, you are many and all very important to me. Thank you!

Samia Oukemeni

Contents

List of Figures

List of Tables

List of Abbreviations

AES	**A**dvanced **E**ncryption **S**tandard
AIC	**A**vailability, **I**ntegrity and **C**onfidentiality
API	**A**pplication **P**rogramming **I**nterface
AQ	**A**ssessment **Q**uestion
CBC	**C**ipher **B**lock **C**haining
DHT	**D**istributed **H**ash **T**able
DoS	**D**enial of **S**ervice
DSA	**D**igital **S**ignature **A**lgorithm
ECIES	**E**lliptic **C**urve **I**ntegrated **E**ncryption **S**cheme
ECDH	**E**lliptic **c**urve **D**iffie–**H**ellman
GQM	**G**oal, **Q**uestion, **M**etric
HTTP	**H**ypertext **T**ransfer **P**rotocol
IEC	**I**nternational **E**lectrotechnical **C**ommission
IPAM	**I**nformation **P**rivacy **A**ssessment **M**etric
IRT	**I**tem **R**esponse **T**heory
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformation **T**echnology
LINDDUN	**L**inkability, **I**dentifiability, **N**on-repudiation, **D**ectectability, information **D**isclosure, content **U**nawareness, and policy and consent **N**on-compliance
MOSNs	**M**icroblogging **O**nline **S**ocial **N**etworks
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
OSN	**O**nline **S**ocial **N**etwork
P2P	**P**eer-to-**P**eer
PAE	**P**rivacy **A**ssessment **E**ngine
PDSA	**P**lan, **D**o, **S**tudy, **A**ct
PGP	**P**retty **G**ood **P**rivacy
PIDX	**P**rivacy risk **I**ndicator
PII	**P**ersonally **I**dentifiable **I**nformation
RSA	**R**ivest–**S**hamir–**A**dleman
SHA	**S**ecure **H**ash **A**lgorithm
SQL	**S**tructured **Q**uery **L**anguage
SSL	**S**ecure **S**ockets **L**ayer
SSN	**S**ocial **S**ecurity **N**umber
SUI	**S**ystem **U**nder **I**nvestigation
TLS	**T**ransport **L**ayer **S**ecurity
TN	**T**rue **N**egatives
TP	**T**rue **P**ositives
URL	**U**niform **R**esource **L**ocator
XSS	**C**ross-**S**ite **S**cripting

List of Symbols

TPS	Total Privacy Score
PPS	Privacy Protection Score
PRS	Privacy Risk Score
N	Total number of questions applicable to the System Under Investigation
N_{Common}	Number of answered questions in case of common set
$N_{Specific}$	Number of answered questions in case of specific set
N_{PP}	Number of answered privacy protection questions
N_{PR}	Number of answered privacy risk questions
N_{NA}	Number of answered N/A questions
$ScoreAQ$	Privacy score calculated for a question
Imp_{Priv}	Privacy impact score
Imp_{Sec}	Security impact score
AV	Accessibility Value
$Diff$	Data Extraction Difficulty

Chapter 1

Introduction

The concept of "Social networking" is not new. It has always existed in different forms and facets [1]. It refers to the act of creating social relationships (e.g. friendship, co-working, acquaintance, etc.) [2] and expanding the social structure of individuals. Online Social Networks (OSNs) are the translation of these physical connections and relationships to the virtual world. The first known OSN was SixDegrees [3], it appeared in 1997. SixDegrees allowed users to create profiles and connect with their friends. The website shut down in 2000.

Online Social Networks can be defined as application systems that represent users and enable them to keep in touch with other contacts [4]. They can be also defined as user-generated content services that allow (i) to create public or semi-public profiles, (ii) to build social relationships with other users, and (iii) to post their activities and interests and view those made by others [5, 6].

OSNs offer a free channel for users to express themselves, to share their thoughts and activities, and to communicate with others. The popularity of OSNs has grown impressively over the years. As of January 2019, the number of users of OSNs reached 2.77 billion monthly active users [7]. This popularity is due mainly to the extended number of functionalities offered in OSNs. They make it easy to share activities, follow interests, chat with friends, upload photos and videos, play games, etc.

The nomenclature of the services might differ from one OSN to another, but the idea behind is the same. Mangold and Faulds [8] categorize social networks based on their similar social characteristics (see Table 1.1).

TABLE 1.1: Classification of Online Social Networks

OSNs category	**Examples**
Social networking	Facebook, Google+
Microblogging	Twitter, Tumblr
Photo sharing	Instagram, Snapchat, Pinterest
Video sharing	YouTube, Facebook Live
Consumer reviewing	Yelp, TripAdvisor
Communication-based	Skype, Viber, Whatsapp
Business networking	LinkedIn, Viadeo
Virtual worlds	Second Life
Advice Sharing	PatientsLikeMe, BabyCenter

OSNs are not limited to a specific demographic or age group, but they encourage people of all ages and demographics worldwide to participate by sharing their thoughts and interests or by advertising their products. The social changes and political movements have added a new role to OSNs. They have become a source of

news coverage and means of propagating all sorts of information. It is quite remarkable how news spread so fast on social networks. For example, OSNs have played a crucial role in the recent events of the 'Arab Spring' [9] or the 'London riots' [10].

1.1 Motivation

OSNs offer various functionalities and services that attract a great number of users to online social services. The users are instantly informed of news of their interests and their entourage. In addition, OSNs can analyze data and correlate users' interests to give advanced and personalized services. They can recommend potential friends or interests based on the information extracted from the users' profiles and activities (preferences, daily browsing, etc.) as well as from their followers' activities. However, having the OSN services managed by a single authority entitles them to some risks of availability and privacy. The Internet shutdowns and servers' failures can be a bottleneck to the traffic and make the services completely unavailable. For example, in March 2019, Facebook, Instagram, and WhatsApp services shut down for several hours and blocked all means of communication [11].

Data published in OSNs are rich in personal and sensitive information. Attackers can gather, aggregate, and exploit the data to commit cybercrimes against the users (e.g. identity theft, phishing, social scams, and social engineering). For example, the website Please Rob Me [12] raises the awareness of the danger of oversharing in social media, especially the information about the geographical location on Twitter. The website scans the feeds from Twitter and shows when the users tweet out locations other than their home.

Furthermore, most of the known OSNs companies handle the users' data and generate their revenue by gathering and selling the data to third-party channels for advertisement or statistical purposes [13]. These companies claim that before selling the data, they anonymize them, meaning that they remove any explicit information from the dataset that can directly identify the users (name, Social Security Numbers (SSNs)...) [14]. However, recent research has indicated that from the anonymized dataset of 1.5 million people, Montjoye et al. were able to identify a person with 95 % accuracy in only four spatiotemporal points [15]. Furthermore, Montjoye et al. [16] studied an anonymized dataset of credit card transactions of 1.1 million people and were able to re-identify 90% of individuals knowing again only four spatiotemporal points. In other words, it is simple and easy to identify a person based on non-identifying attributes (sex, birthdates..) other than the ID. Hence, anonymization is not a sufficient approach to protect the users and the privacy of data is in jeopardy when it is placed in the hand of online companies.

As the monetary value of data increases, more voices demand protection and control over their privacy. The year 2018 saw a trend to enact new laws that regulate data collection and enhance privacy protection. For example, the European Parliament approved the General Data Protection Regulation (GDPR) on 14 April 2016 to be applied by 25 May 2018 [17]. The new regulation aims to give control to online users over their personal data, to harmonize data privacy laws across Europe, and to protect the privacy of the users [18]. However, GDPR is not the miraculous solution to protect the users' privacy. In fact, the end users have to accept the terms and conditions as provided by the system, they are not in a position to negotiate a separate agreement. Therefore, the users are obliged to accept to release their data as a necessity to use the services [19]. Moreover, the regulation was criticized for the lingering uncertainty around some undefined terms (e.g. "disproportionate effort"

or "undue delay") which require more clarity by the courts and regulators. Furthermore, GDPR does not offer a proper definition of what constitutes a "reasonable" level of protection for personal data, offering flexibility in the assessment of fines for data breaches and non-compliance [20].

In recent years, various privacy-related scandals have come to light regarding the misuse of personal data. One of the most important was in 2018. A former Cambridge Analytica contractor admitted that the firm harvested more than 50 million Facebook profiles without permission to build an algorithm that targeted US voters with personalized political advertisements based on their psychological profile [21]. The data was collected through an app called "thisisyourdigitallife", built for academic purposes [22]. The Cambridge Analytica scandal has generated a wave of general anger directed at Facebook's poor management of users' privacy, resulted in a Twitter campaign under the hashtag #DeleteFacebook, calling on users to delete their Facebook accounts. However, it seems that relatively few Facebook users have actually deleted their accounts. The number of monthly active Facebook users have jumped from 2.19 billion users in the first quarter of 2018 to 2.38 billion users in the first quarter of 2019 [23].

The contradiction between releasing data and the concern about the protection of privacy is called "the privacy paradox" [24]. A great number of users of OSNs are aware of the importance of protecting privacy [25]. They claim that they understand the risk of releasing private data. But at the same time, they accept to disclose data as a price to benefit from the services. The most plausible psychology explanation to this phenomenon is that the users understand the tradeoff between losing privacy and the benefits they get from using the OSNs services and they regard the latter as outweighing the former. Even experienced users who are aware of their privacy risks are sometimes willing to compromise their privacy in order to improve their digital presence in the virtual world. That is, they prefer being popular and "cool" to being conservative with respect to their privacy. They know that the loss of control over their personal information poses a long-term threat, but they cannot assess the overall and long-term risk accurately enough to compare it to the short term gain. Also, they often do not have the expertise needed or the adequate tools to protect their privacy nor to understand what are the potential consequences if privacy is violated. The reason for this is because privacy concern is an abstract feeling and hard to express in specific terms. Privacy itself is an intuitive term that can be interpreted differently depending on the culture or the situation. The sense of what should be kept private and what should be public changes from one person to another and from one culture to another [26]. Even in the same situation, two individuals may act differently depending on what privacy means to them.

1.2 Purpose and Scope of the Thesis

Due to the exponential development of information technologies, protecting privacy becomes extremely important, especially in the field of social media and microblogging services. OSNs have brought new challenges to privacy-oriented companies and the academic community. Researchers have discussed new privacy-preserving controls and techniques and they have proposed different techniques and new systems to protect and enhance the users' privacy. As the definition of privacy is ambiguous and elusive, there are no standard means of how to build an efficient privacy-protecting system.

The abundance of privacy preserving strategies and online social networks comes with a difficulty to quantify each system and measure its level of privacy provided to protect the personal information of users. Therefore, a formal framework is needed to compare online social networks and assess their degree of privacy. OSN developers can use such a framework to evaluate the performance and efficiency of the privacy-preserving techniques used in systems. Also, the framework will be useful for the end users to choose which platform is more adequate for their needs and requirements in terms of privacy, especially that they do not have enough information to understand the privacy implications of using some services on online social networks.

In this thesis, the focus is on providing privacy metric to evaluate and assess the level of privacy of OSNs that offer, but not exclusively, microblogging services. Microblogging is a weblog that allows a small number of characters for each post (between 140 and 310 characters for most of the existing microblogging systems) [27].

Microblogging services provide light-weight and simple means to share and publish information about life, activities, interests, opinions, news, current events, etc. It is a fast and easy mode for communication. Comparing with regular blogging systems, the short-nature of messages in microblogging systems shortens the time needed to post messages, allowing users to post several messages in a single day. For example, Twitter is a popular microblogging system [28] where the number of monthly active users exceeds 330 million users in the first quarter of 2019 [29].

1.3 Objectives of the Thesis

The main objectives of the present thesis are:

- **O1. To investigate how privacy can affect the information sharing behavior of users in OSNs.** More specifically, to examine the factors that influence how users share their personal information on social networks and how they perceive privacy in OSNs. The analysis helps to determine the preferences and requirements of users for an ideal OSN system that provides social functionalities while preserving privacy.

- **O2. To review the state of the art of OSNs that offer, but not exclusively, microblogging services.** The systems can be either proposed in the literature or deployed and used by real users. The analysis will help in identifying and extracting common features and characteristics of microblogging systems. These characteristics lead later to compare different systems and measure their level of privacy.

- **O3. To propose and design a framework to evaluate the privacy level of microblogging systems.** The privacy scores obtained from using the proposed metric will be used by the end users to choose which microblogging system is more adequate for their needs in terms of privacy requirements. It can be also used by systems' providers to evaluate the efficiency and effectiveness of the privacy mechanisms implemented in their systems.

- **O4. To compare the previous surveyed systems according to their obtained privacy scores.** The study will be used to investigate the feasibility of the proposed privacy scoring framework.

It should be noted that the study of methods and technologies to extract and gather information used in privacy metrics is beyond the scope of this thesis.

1.4 Research Methodology

The present work was carried out using 4 different research methodologies. First, an extensive and a comprehensive literature review on privacy enhancing techniques and microblogging systems was conducted using *Literature Review* [30] as research methodology. Second, we used a questionnaire *Survey* [30] as research methodology to understand the perception of users towards privacy in OSNs. Third, a framework was created and developed to evaluate and quantify privacy level in microblogging OSNs using *Design and Creation* research methodology[30]. Fourth, a series of *Experiments* [30] was conducted to evaluate and validate the proposed framework.

1.5 Main Contributions

This thesis provides several novel contributions to the field of privacy scoring in microblogging Online Social Networks.

- **C1.** *Designing and conducting an online questionnaire survey intended for Online Social Networks' users.* The survey aimed to analyze the perspective of the OSNs' users on the ongoing situation of privacy protection in OSNs and their effect on information sharing behavior. This contribution addresses the objective **O1** and discussed in details in Chapter 3. The analysis and results are submitted to the journal "*Behaviour & Information Technology*" [1] **[P2]**.

- **C2.** *Conducting a literature review and a comparative analysis of the state of the art of the existing social network systems, with a special focus on microblogging systems (e.g. Twitter, Diaspora, etc.).* The analysis helped in identifying the common characteristics of microblogging systems in terms of features, design, security requirements, and privacy-enhancing techniques implemented in microblogging online social systems. The results helped also in understanding the privacy issues that such services are suffering from. This extensive research aims as well to gather data on the internal work of the microblogging systems in order to identify privacy enhancing techniques implemented in online social systems. This contribution addresses the objective **O2** and discussed in details in Chapter 4. The results of the comparative analysis are published as a technical report at UOC - Garlanet's web site [2] and as a survey article in the journal *ACM Survey Computing* [3] **[P1]**.

- **C3.** *Designing and developing information privacy assessment metric (the IPAM framework).* The aim of the framework is to quantify, assess and evaluate privacy level in microblogging OSNs. First, we presented a systematic methodology to develop privacy metrics in microblogging OSNs based on the Plan-Do-Study-Act (PDSA) cycle. Second, we defined a privacy scoring metric that is based on the impact of privacy and security requirements, accessibility, and difficulty of information extraction. This contribution addresses the objective

[1] https://www.tandfonline.com/toc/tbit20/current
[2] http://dpcs.uoc.edu/projects/garlanet/files/technical-report-privacy.pdf
[3] https://csur.acm.org/

O3 and discussed in details in Chapter 5. A general overview of the architecture and the methodology of the framework was presented in *XV RECSI workshop* [4] **[P4]**. A more detailed version of the article is published in the journal *IEEE Access* [5] **[P3]**.

- **C4.** *Evaluating the performance and efficiency of the proposed framework*. The analysis consisted of comparing the systems surveyed in the previous step to determine their privacy level based on the scores obtained from the IPAM framework. This contribution addresses the objective **O4** and discussed in details in Chapter 6.

1.6 Outline of the Thesis

The rest of this thesis is structured as follows:

- Chapter 2 summarizes the preliminary concepts and background information used in the rest of the thesis. It includes an overview of the state of the art in privacy metrics in the field of OSNs.
- Chapter 3 presents the results of the conducted online questionnaire survey to understand and analyze the attitude of users towards privacy and how they behave about information sharing in OSNs.
- Chapter 4 contains a comparative analysis study to evaluate 24 different Online Social Networks(OSNs) based on a set of characteristics, and to compare them based on their usability and the level of protection of privacy they provide.
- Chapter 5 introduces an information privacy assessment metric to quantify, assess, and evaluate privacy in microblogging OSNs.
- Chapter 6 presents a quantitative comparison of microblogging OSNs surveyed in chapter 4, using the algorithmic model proposed in chapter 5.
- Finally, Chapter 7 concludes the thesis and presents guidelines for future work.

Figure 1.1 depicts the structure of this thesis and maps the chapters to their respective objectives and articles.

[4] https://nesg.ugr.es/recsi2018/
[5] https://ieeeaccess.ieee.org/

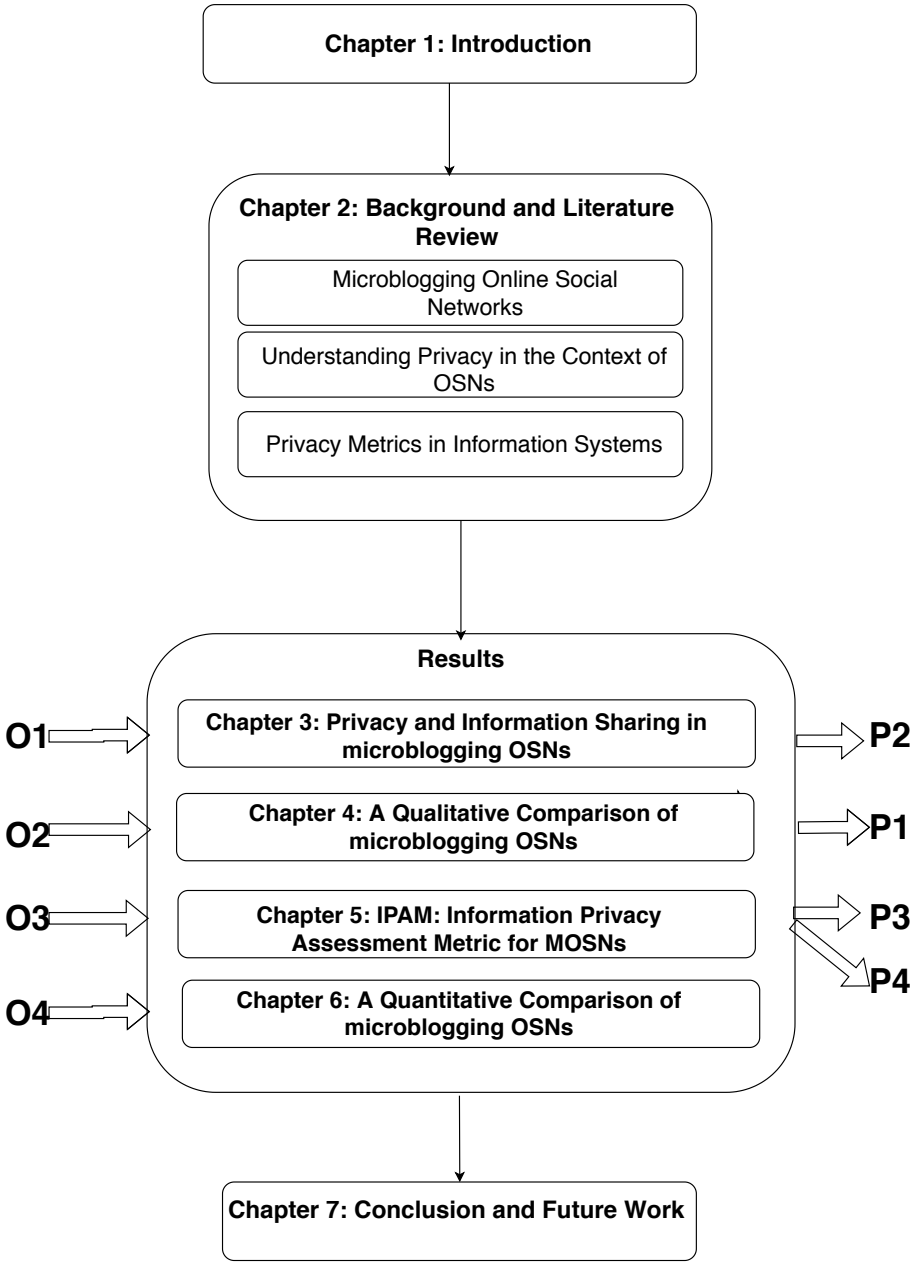


FIGURE 1.1: Thesis Outline

Chapter 2

Background and Literature Review

This chapter recalls some concepts and related works representing the background necessary to understand the rest of this research thesis. This chapter is structured as follows: Section 2.1 introduces Microblogging Online Social Networks (MOSNs). Section 2.2 defines the concept of privacy and presents its principles and objectives. Section 2.3 explains some privacy threats and attacks in the context of MOSNs and how to mitigate them. Section 2.4 presents the state-of-the-art in privacy metrics in Online Social Networks. Section 2.5 concludes the chapter.

2.1 Microblogging Online Social Networks

As defined in the introduction 1, microblogging is a popular form of Online Social network. It differs from traditional blogging mainly because users can broadcast their interests and activities in the form of snippets of a small number of characters, in general between 140 and 310 characters for most of the existing microblogging systems [27].

Microblogging systems offer to their users the ability to create customized profiles, follow and be followed by friends and acquaintances, share interests and keep updated with the trending topics and news [31]. The users might include in their post pictures, URL links, video links, etc. They can also keep track of activities from other friends/followers, trends, companies, brands, and celebrities [32].

When studying MOSNs, there are two major aspects that characterize them: the targeted stakeholders involved in the usage of microblogging services and the data used and collected in the system [33, 34].

2.1.1 MOSNs Stakeholders

MOSNs stakeholders are defined as entities that can access user-data directly or indirectly. They can be categorized into users, service operators, third-parties, and the general public.

- **User**: is any entity (an individual or an organization) that subscribes to an MOSN to benefit from the services offered [33]. A user is represented by a profile, her relationships, and her generated contents.
- **System operator** (also known as service provider): provides the underlying services and infrastructure needed to use the system and interact with each other [33]. They play the role of data protectors, and they can have direct or indirect access to the user data.
- **Third-parties**: are entities that connect to either system operators or users for different objectives other than social networking [33]. They can be developers

of applications, providers of add-ons, data analysts, marketers, advertisement agencies, etc.

- **General public**: are unregistered users that can access (if they are allowed) to the services of the OSNs to visualize, monitor, or extract information.

Figure 2.1 illustrates the stakeholders in MOSNs. The direction of the arrows shows the flow of the data between the stakeholders.

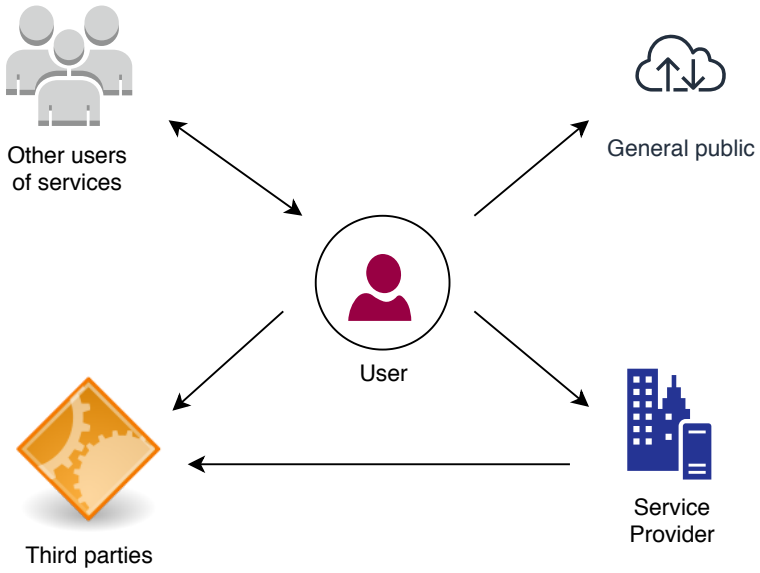


FIGURE 2.1: MOSNs stakeholders

The next section identifies the types of data circulated between the stakeholders in MOSNs.

2.1.2 MOSNs Data Types

The user data are either provided in the user's profile, generated by the user, shared in groups, collected from patterns, or derived from all the other types of data. Kumari in [33] classifies the user data into two categories:

- **Traffic data**: all data generated from users' activities, such as IP address, OS specifications, search terms, etc.
- **Payload data**: all data posted by the user herself or posted about the user by other users.

Furthermore, the payload data can be classified into [35]:

- **Service data**: are the data the users give to a social networking site in order to use, like name, age, email address...
- **Disclosed data**: are the data generated by the users in their own pages.
- **Entrusted data**: are the data that a user posts on other people's pages, like commenting on friends' messages, photos, and videos, tagging friends in photos, etc.

- **Incidental data**: are the data posted by other users about the user. It is basically similar to the entrusted data, but the user has no control over the data posted. They can include comments on user's photos and videos, comments on the user's status updates', etc.
- **Behavioral data**: are the data collected about the users' habits and activities.
- **Hidden or derived data**: are the data derived from all the other types of data.

The data categories are illustrated in Figure 2.2:

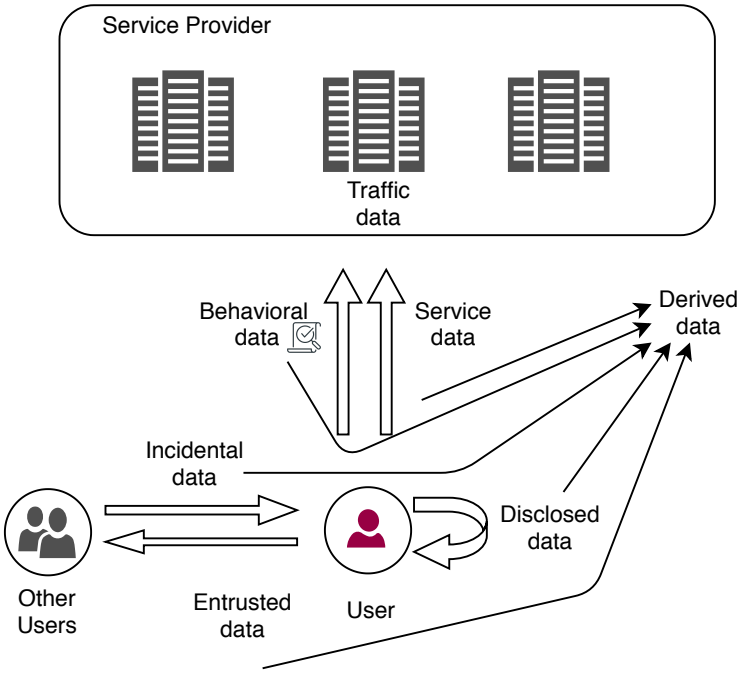


FIGURE 2.2: MOSNs data types

2.2 Privacy

Privacy is recognized internationally as a fundamental human right [36]. However, in this data-driven world, protecting privacy becomes one of the dominant issues, as it is threatened by the terabytes of personal information revealed every day.

According to Oxford dictionary [37], privacy is defined as:

> " A state in which one is not observed or disturbed by others".

From the definition, we can see that the concept of privacy is an intuitive term, yet not easy to define. The term is ambiguous and what it should be kept private and what must be revealed changes from one person to another [26].

Privacy has many meanings depending on the culture, the society, or the discipline's perspectives, i.e. law, health sciences, social sciences, and computer and information science, yet no single definition of privacy encompasses all aspects of the term.

There are three (3) main dimensions from which the privacy is described and analyzed: legal, social and technical perspectives [38].

1. **Legal dimension**: privacy is a right that needs to be protected by laws, regulations and policies [39]. It is defined as a set of policies that enforce the protection of private information [40].

2. **Social dimension**: privacy depends on the behavior and the interactions of individuals as they conduct their daily affairs [38]. Rachels [41] explained that

   > "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have".

   In such a way, privacy proves to be evolving with cultural changes and technological advances.

3. **Technical dimension**: the technical dimension aims to protect privacy through technical specifications by controlling (automatically and/or manually) data and information. This dimension is concerned with how the legal and social understandings of privacy can be represented and implemented in systems. Westin [42] defined information privacy 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". He added to this definition [43] "the right to determine when data are obtained and what uses will be made of by others". Bünnig et al. [44] described privacy as protecting personal information from malicious and unauthorized entities. Another definition of privacy is to hide some details from others [45].

When talking about privacy in OSNs, it revolves mostly around information privacy. In the traditional web, information privacy is controlled by limiting data collection, granting access to authorized entities and by hiding the user's identity. These solutions may not address the new privacy challenges created by OSNs where a user openly and willingly shares a whole data set of personal information in the profile [46]. Due to this trade-off between the open nature of OSNs and the sensitivity of published data, the concern about the privacy issues in OSNs is raised and the protection and management of privacy in OSNs are a lot harder.

2.2.1 Privacy Laws and Principles

Information privacy laws and regulations deal with protecting any personally identifiable data collected by any entity (public/private organizations or other individuals). There are multiple information privacy laws and regulations available defined by different organizations and countries. In addition, several privacy principles have been adopted to ensure the protection of privacy. In the following, we review some known laws and regulations of information privacy.

OECD

The Organization of Economic Cooperation and Development (OECD) organization [47, 48] provides the most commonly used privacy framework. The privacy principles are reflected in existing and emerging privacy and data protection laws and serve as the basis for the creation of leading practice privacy programs and additional principles. The OECD privacy principles include 1. collection limitation, 2. data quality, 3. purpose specification, 4. use limitation, 5. security safeguards, 6. openness, 7. individual participation, 8. accountability, and 9. free flow and legitimate restrictions.

GDPR

General Data Protection Regulation (GDPR) is a European regulation (2016/679) on data protection and privacy for all individuals within the European Union. The regulation becomes applicable as of May 25th, 2018 in all member states. It aims to harmonize data privacy laws across Europe and it is applicable to any business that holds or processes the personal data of EU citizens, regardless of their location [18]. GDPR provides seven privacy principles [49, 50]: 1. lawfulness, fairness and transparency, 2. purpose limitations, 3. data minimization, 4. accuracy, 5. storage limitations, 6.integrity and confidentiality, and 7. accountability.

PIPEDA

Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law relating to data privacy that governs the private sector [51]. PIPEDA outlines ten privacy principles to follow: 1. accountability, 2. identifying purposes, 3. consent, 4. limiting collection, 5. limiting use, disclosure, and retention, 6. accuracy, 7. safeguards, 8. openness, 9. individual access, and 10. challenging compliance.

ISACA

Information Systems Audit and Control Association (ISACA) is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management, and governance [52]. The ISACA privacy principles outline core principles used to ensure data privacy protection [53]: 1. choice and consent, 2. legitimate purpose specification and use limitation, 3. personal information and sensitive information life cycle, 4. accuracy and quality, 5. openness, transparency and notice, 6. individual participation, 7. accountability, 8. security safeguards, 9. monitoring, measuring and reporting, 10. preventing harm, 11. third party/vendor management, 12. breach management, 13. security and privacy by design, and 14. free flow of information and legitimate restriction.

ISO/IEC 29100:2011

It provides a privacy framework that specifies a common privacy terminology and defines the actors and their roles in processing personally identifiable information (PII) [54, 55]. It describes privacy safeguarding considerations and provides references to known privacy principles for information technology.
ISO/IEC 29100:2011 is applicable to organizations where privacy controls are required for the processing of PII. The privacy principles outlined by ISO/IEC are 1. consent and choice, 2. purpose legitimacy and specification, 3. collection limitation, 4. data minimization, 5. use, retention, and disclosure limitation, 6. accuracy and quality, 7. openness, transparency and notice, 8. individual participation and access, 9. accountability, 10. information security, and 11. privacy compliance.

Table 2.1 provides mapping and comparison between different privacy principles in information privacy laws and regulations. The terminology might differ, but the basic privacy principles of data protection are almost the same.

The common privacy principles between the cited laws and regulations are :

- Purpose specification ensures that the data controllers should describe and specify the purpose(s) for which the data is collected.

TABLE 2.1: Information privacy laws and regulations

Privacy Principles	**OECD**	**GDPR**	**PIPEDA**	**ISACA**	**ISO**
Common Principles					
Consent		✓	✓	✓	✓
Purpose specification	✓	✓	✓	✓	✓
Data collection and minimization	✓	✓	✓	✓	✓
Accuracy	✓	✓	✓	✓	✓
Limitation of use	✓	✓	✓	✓	✓
Accountability	✓	✓	✓	✓	✓
Information security	✓	✓	✓	✓	✓
Specific Principles					
Openness and transparency	✓	✓	✓	✓	✓
Individual participation	✓	✓	✓	✓	✓
Monitoring and enforcement			✓	✓	✓
Third party management				✓	
Breach management				✓	
Security and privacy by design				✓	
Free flow of information	✓	✓		✓	
Preventing harm				✓	

- User consent should be explicitly obtained prior to collecting, transferring or using data.
- Data minimization and collection limitation ensure that the data collection is limited to the purposes identified and what is necessary.
- Accuracy ensures that the data is accurate, complete, and up-to-date.
- Limitation of use of data ensures the appropriate mechanisms the data is disclosed, retained and deleted.
- Accountability ensures that someone is accountable for the management of data and adheres to due diligence and concrete measures for its protection.
- Information security ensures that data is protected with appropriate security safeguards.

Most of the discussed laws and regulations are geographically limited to the national level of the applied countries. Furthermore, there is no explicit law or regulation specific to regulate the domain of OSNs. The laws and regulations are also vague about what measures and safeguard the organizations should take to ensure the implementation of the principles. In addition, the cited principles allow agencies and organizations to use private data for monetary purposes as long as the purpose of the collection is clearly indicated and the consent is obtained from the users.

2.2.2 Privacy Objective and Requirements

Working with protection requirements is familiar in IT-security sector. They are developed to meet the demands of technical and organizational measures to achieve the desired level of protection and to assess the risks and investigate potential threats.

Information security refers to the protection of all types of information and systems [56]. The protection of information security relies mainly on three crucial principles or what is known as AIC-triad (Availability, Integrity, and Confidentiality). AIC-triad is a model designed to guide the integration of IT security protection mechanisms within an organization [57]. The meanings of these three goals vary depending on the context and the environment of the organization (policies, laws, regulations...) and each asset requires a different level of protection of each of the three AIC goals against IT threats and vulnerabilities [58, 59]. The AIC-triad can be defined as [57, 59, 60]:

1. **Availability** ensures the access to authorized data and resources at any time and from everywhere.
2. **Integrity** ensures the reliability of the data, stored or in transit, and guarantees that any unauthorized modification is blocked.
3. **Confidentiality** protects the data content and prevents any unauthorized disclosure.

If the information security requirements are universally accepted and considered crucial to evaluate the security status in any IT system, the requirements of information privacy are still new and not yet common or well established. In this aspect, research has tried to come up with formalized models for privacy requirements. In the following, we present 3 sets of privacy requirements.

LINDDUN and PriS Method

LINDDUN [61] and PriS Method [62] are composed of eight privacy goals or requirements to achieve the users' privacy protection:

1. **Anonymity** can be defined as the impossibility of identifying a subject within an anonymous set of subjects [63].
2. **Pseudonymity** refers to the possibility of using multiple pseudonyms by the same subject for different purposes. For instance, the same subject can post messages in a microblogging system under a pseudonym different than the one used to send emails [63].
3. **Unlinkability** refers to hiding the link between two or more pieces of information (identities, actions...) [63].
4. **Unobservability** refers to hiding the relationship between two activities of the same user [63].
5. **Data protection** or confidentiality is defined in security requirements and it can be achieved using encryption.
6. **Plausible deniability** refers to the ability to deny performing an action or producing a piece of information[63].
7. **Intervenability** refers to the right of individuals to rectify, erase and withdraw their data from the system's databases [58].
8. **Censorship-resistance** prevents system's provider from denying access to a particular piece of information (file, resource...) and ensures that the information is accessible to all authorized users anytime and anywhere [63] [64].

EuroPriSe Privacy Requirements Set

The set was proposed in 2009 [65]. It was further refined in [66, 67]. It was embedded in a standardized data protection model and proposed for use on the European level. It defines three privacy-specific protection requirements namely:

1. **Unlinkability** ensures that privacy-relevant data cannot be linked to any other privacy-relevant information outside of the domain. To achieve unlikability, mechanisms like separation of contexts, anonymization, and pseudonymization can be used.

2. **Transparency** ensures an adequate level of clarity of how privacy-relevant data are processed. For example, reporting mechanisms, organization and responsibilities, and privacy policies can be used to achieve transparency.

3. **Intervenability** aims at the possibility to interfere with data processing by the parties whose data are processed. This requirement is less technical. For example, allowing users to change settings, changing to non-personalized recommendations are ways to achieve Intervenability.

NIST Privacy Requirements Set

The set of privacy requirements is proposed by the National Institute of Standards and Technology (NIST) [68]. In addition to the 3 security requirements (AIC), NIST has defined three (3) privacy requirements [69]:

1. **Predictability** aims at building trust and accountability between the system and the users about how the privacy-related data are processed. Predictability can be met with technical solutions such as logging and reporting.

2. **Manageability** provides the capacity to administer personal information including editing, deleting, and selecting disclosure.

3. **Disassociability** aims at protecting an individual's identity and associated activities from disclosure and ensures that processing of personal information is disassociated to individuals.

2.2.3 Defining Privacy in MOSNs

We set the concept of privacy in OSNs by embracing the previous definitions in the context of MOSNs and defining privacy as the right to:

- decide what information to publish and who can access it.
- manage data (edit, download, and delete data at any point in time).
- assess the use, the processing, and the dissemination of data (who, how, what).
- give consent before any collection, use, or disclosure of data.
- specify the minimum acceptable of data in the system to provide the services.
- choose where to store data (locally or using the system's servers).
- protect all data available on the system from inquisitive entities.

Our definition of privacy in MOSNs captures, in essence, the idea of providing the users with the guarantee of data protection and with the autonomy (i) to assess the use and the access to data, (ii) to take appropriate action to protect their privacy, and (iii) to be assured that privacy is enforced and protected by the system.

2.3 Understanding Privacy in the Context of OSNs

In traditional online services, information privacy is carried out through technical specifications by controlling (automatically and/or manually) access, limiting data collection, and hiding users' identities. However, in the case of OSNs, data and identities are linked and usually revealed to the public ([70]). While users are encouraged to share and improve their digital presence in the virtual world, many are becoming more aware of the information privacy breaches present in the OSNs. Next, we discuss main privacy threats and attacks present in MOSNs, and we explain some techniques to mitigate them.

2.3.1 Privacy Threats in MOSNs

With the increasing popularity, microblogging systems, and online social networks in general, have become a hub for cybercriminal activities. Attackers and malicious users are drawn to these platforms and specifically to the sensitive data disclosed, intentionally or unintentionally, by the users. Most of the attacks are driven by the purpose of harassment, identity theft and stealing information related to bank accounts or social security numbers [71].

Some privacy risks are more amplified in MOSNs compared to traditional service systems. These include:

- Malicious insiders can connect with the victims and act as legitimate users.
- User can unintentionally disclose personal information, like geographic location, interests, etc.
- Joint utilization of different OSNs can bring in a new type of attacks based upon the fusion of multiple profiles of the same user across multiple OSNs.
- Third-party applications can use the API provided by the MOSNs and access users' profiles. Also, these applications may have vulnerabilities that attackers can exploit to get to the users' accounts. For example, a vulnerability in Twitter Counter, a popular tool for analyzing Twitter followers, was exploited in 2017, which has led to taking control of hundreds of high-profile Twitter accounts like the European Parliament, UNICEF, and Amnesty International [72].

There are two different categories of privacy threats: (a) user-related threats generated from the disclosure of published data to other users (whether registered or not) and (b) system provider-related threats generated from the system (such as private information, location details, IP address, behavioral activities). The difference between the two types of threats is the kind of data that can be accessed and, consequently, each category requires its own specific defense mechanisms.

User-Related Threats

They revolve around sensitive data disclosure to other OSNs users or unregistered users. Privacy breaches can be either intentional (e.g. hacking) or unintentional (e.g.

misconfiguration of privacy settings). Several threats may be included under the user-related threat category [73, 74, 75, 76]:

- Inability to hide information from other users due to design flaws in the system, or due to the unawareness of the existing privacy settings.
- Inadequate configuration of the present privacy settings, which may lead to disclosing sensitive information.
- No control over what other users may publish (e.g., labeled photos, mentions, comments).
- Using machine learning algorithms, an adversary may disclose and predict non-explicit data.
- An adversary may analyze the feeds and disclose the hidden relationship between the users.
- An adversary may complete the profiling of a user via a secondary data collection from different OSNs.

System Provider-Related Threats

When registering in an OSN, the user implicitly puts its trust in the system provider to handle and protect the data in fairness and accuracy. However, the OSNs have full access to a large amount of data, including browsing behavior, metadata (e.g. users' operating systems, browsers, IP addresses), logs, etc. Using this data, the system provider can perform data mining techniques and extract further implicit data that might violate the user's privacy. Some threats that fall under this category are [73, 74]:

- The collected data by the OSN is more than the minimum needed for a user to interact with the services.
- The system does not provide the right to be completely removed from the system.
- Third parties are interested in the profiles of OSN users and their data.
- OSNs are vulnerable to specific attacks (like Sybil attacks [77] or social spamming [78]) as well as the typical cyberattacks of any online service (DoS, SQL injection, XSS, social spamming, flooding, phishing and malware attacks [71]).

2.3.2 Privacy Attacks in MOSNs

The popularity of microblogging systems such as Twitter has attracted attackers and malicious users to target these online communication services and specifically the critical data gathered and displayed on these platforms. Most of the attacks are driven by the purpose of harassment, identity theft and stealing information related to bank accounts or social security numbers [71]. Privacy attacks in MOSNs can be categorized into two categories: (1) classic attacks and (2) MOSN related attacks.

Classic Attacks

Like any online platform, MOSNs are vulnerable to classic attacks [71] [79].

- **SQL injection** is a traditional form of attack. It consists of inserting an SQL query via the input data. A successful SQL injection can read sensitive data from the database and modify or delete database data [80]. This attack affects the availability, confidentiality, integrity of the data, and the reputation of the system.
- **Cross-Site Scripting (XSS)** is one of the most common web application attacks where adversaries introduce an illicit scripting code into the application code. In the case of OSNs, XSS worms are injected in the form of posts to hijack user's accounts and steal sensitive information of the user [81, 82]. It threatens the protection and integrity of data and the integrity of the system.
- **Denial-of-Service attacks (DoS) and Distributed Denial-of-Service attacks (DDoS)** are traditional forms of attacks. The OSN is sent a large number of requests that overload the service and deny access to it [83]. It affects the availability of the system.
- **Malware** is a program that gains access, disrupts normal services, gathers sensitive information, or damages the system. Malware propagation is rapid due to the trust relationships in social networks [83]. The kind of attacks disturbs the availability and integrity of the system and data protection.
- **Social spamming and phishing attacks**: Social spamming depends on the access control of the users and the level of accessibility of data. They can be either Well-defined targeted spams or Broadcast spamming [78]. A phishing attack targets the confidential information provided in the OSN. The adversary attempts to acquire sensitive information from a victim by impersonating a trustworthy third party. It is usually combined with social spams to achieve total success [84, 78].

MOSN-Specific Attacks

With the increase of demand for MOSNs, specific attacks have been developed for such platforms.

- **Conversation and communication tracking**: the adversary tracks the communication feed of users and collects information about the user by searching the posts and the comments left by other users [75].
- **Crawling and harvesting**: the adversary is not interested in one particular user, but in collecting and aggregating available information across the profiles in the OSN. This information can be used for users' activities analysis or in marketing advertising. Harvesting is when the adversary uses multiple OSNs platforms to collect and aggregate private information [75, 85].
- **De-anonymization attacks**: they refer to the process of reversing the anonymization and de-identification performed by the system provider before publishing/selling the data. De-anonymization discloses any personally identifiable information and links the data to users. It can be achieved using prior or background knowledge [86]. It includes also group de-anonymization attack [87].

- **Identity theft**: it's an illegal use of personally identifiable information (PII) without the consents of the owner. The adversaries use the stolen ID to authenticate themselves in the system and impersonate the victims [88], then the victims cannot create an account on the system since the ID is already taken.

- **Image retrieval and analysis**: free access to images and digital contents has a risk on the privacy of the users. Image retrieval and analysis are automated attacks that aim to collect multimedia data available on OSNs. Usually, it is followed by pattern recognition to find the links between the OSNs profiles and real users. The multimedia data can reveal more private information about users (friends, education, habits, visited locations,...)[75].

- **Information leakage and disclosure**: the information shared via social networks can be extracted by the adversary or service provider for various purposes (fraud, spamming...). Information leakage may sometimes lead to inference attacks in which the attacks try to disclose the user's unrevealed information [71]. This type of attacks includes attribute disclosure [76], social link disclosure and prediction [76], and affiliation link disclosure [76].

- **Malicious activities**: this type of activities includes profile hijacking and brandjacking [75], fake friendship requests [75], clickjacking attacks [71, 89], social media fraud [71, 90], malicious contents and URLs [91], and group metamorphosis [75].

- **Social engineering attacks**: the adversary uses techniques like phishing, spams, fake profiles, etc. to psychologically manipulate an unsuspecting person into divulging sensitive details and infiltrate networks and obtain data and access [92].

- **Social profiling**: It refers to the process of collecting information and constructing a user's profile. This occurs through aggregating information that is publicly and voluntarily shared social data in OSNs [93, 94]. Social profiling depends on the visibility of data in the profiles and it threatens the anonymity of the users.

- **Sybil attacks**: the adversary attempts to create multiple identities to make as many friends as possible with legitimate accounts. With a Sybil attack, the power and the influence of the adversary increases in the network and thereby engages in malevolent activities like spamming, identity fraud, clickjacking [77]. Fake profiles are also created to increase the visibility of the content and manipulate the view counts[95].

2.3.3 Privacy Mitigation Techniques

Given a large amount of sensitive information exposed on MOSNs and the multiple threats that the systems suffer from, the challenge is to provide the correct techniques and tools to protect the user's information from others and from the MOSN provider itself while taking full advantage of social networking services. This challenge translates into the need for efficient and adequate mitigation techniques to protect privacy in MOSNs.

- **Anonymization.** MOSNs providers often sell user's information to advertising or to third party partners. The data selling is the foundation of the business

model for many OSNs and major revenue sources for the providers. To mitigate the privacy issues, the MOSNs providers tend to anonymize the data by removing any "personally identifiable information" (PII) that can link the user to the anonymized data. However, multiple re-identification attacks [96, 87, 97] can be launched to find the missing information from the anonymized data.
More comprehensive anonymization techniques are proposed to alleviate re-identification issues. For example, Hay et al. [98] proposed random perturbations in order to achieve identity obfuscation in social graphs. Another technique for anonymization is k-anonymization [99, 100], where for every user there are at least $k-1$ other users with the same degree. Differential privacy [101, 102, 103] is another approach for anonymization. The main idea of differential privacy is to add noise to a dataset so that an adversary cannot decide whether a particular piece of information is included in the dataset or not.
Anonymization is an excellent approach to prevent data breaches and disclosures from data selling. However, MOSNs are complex systems and it is hard to prevent data from being combined with additional information retrieved from external sources and recover the anonymized data.

- **Decentralization.** As a solution to mitigate the access of MOSNs to users data is to design decentralized architectures for managing users information, hence reducing or eliminating altogether the centralized view of the system over the users' data. Decentralization removes the issue of lack of trust in MOSNs and the abuse of authority in data handling.

  Most of the decentralized MOSNs use distributed hash tables over unstructured overlays to guarantee the performance [104]. The systems use data encryption and give access to only authorized users.

  Decentralization is used to control and enhance user privacy and to lower the cost of the provider [105]. However, decentralization in MOSNs requires appropriate mechanisms to distribute the storage and to update data, means to search for friends and contents, and ways to be open and adaptable for third-party applications [105].

  Decentralized platforms give a perfect solution to the untrusted systems. But, they should take into consideration the untrusted peers and the technical feasibility for providing availability and integrity of data.

- **Encryption.** An approach to mitigating privacy issues in MOSNs is to shift the access control from all users and/or service provider to only authorized users using encryption. It can provide confidentiality and integrity, and it can be coupled with decentralization and fine-grained privacy settings.

  Jahid et al. [106] proposed EASiER to mitigating the challenge of key management in OSNs. EASiER is a fine-grained access control architecture for OSNs that uses Attribute-Based Encryption (AB encryption) [107]. The users encrypt profile information and posts with attributes policies. Only the authorized users with enough attributes to satisfy a policy can decrypt the data. EASiER provides revocation without issuing new keys using trusted proxies. The proxy uses its proper keys to convert ciphertext into a form that an unrevoked user can combine with its secret key and decrypt the ciphertext, whereas a revoked user can not.
  Using encryption as an attempt to protect privacy in MOSNs is not as easy as

it seems, it brings important challenges. A proper encryption scheme should be chosen. There should be a clear mechanism of key management and distribution and it must be clear which data to encrypt and where to store it.

- **Information security.** Privacy and security are inseparable, they have this cooperative interdependent relationship between the two concepts.

  In addition to encryption that provides confidentiality, safety measures should be applied to mitigate against security attacks. MOSNs providers should ensure authentication and data integrity and keep users' data consistent. Authentication prevents an adversary from accessing hijacked accounts and publishing false information. For example, the authentication mechanism can be applied using multi-factor authentication [108, 109]. In addition, MOSNs providers need to ensure availability of data published by users. Furthermore, MOSNs need to implement internal mechanisms to protect the system against spams, fake profiles, phishing, and other threats. Lee and Kim [110] proposed Warningbird to detect suspicious URLs on Twitter. Whereas Aggarwal et al. [111] presented the PhishAri to mitigate phishing attacks on Twitter. The technique detects whether or not a tweet posted with a URL is phishing using Twitter based, URL based, and WHOIS based features. Bhat and Abulaish [112] designed a framework that uses OSNs community-based features to learn classification models and identify spammers in OSNs. Cao et al [95] presented a tool called SybilRank that ranks users based on the likelihood of being fake using OSN social graph properties.

- **Fine-grained privacy settings and access controls.** Given the huge amount of sensitive information shared daily in MOSNs, the challenge is to provide adequate tools to protect the users and their data from exposure and disclosure while taking full advantage of social networks. This challenge can be translated to give the users more control over their data using fine-grained privacy settings to manage the visibility and the acceptability to data.
  Baatarjav et al. [113] proposed a privacy management system to recommend privacy settings and to predict the users' preferences based on provided profile information by the users. A privacy wizard proposed in [114] is based on the user's privacy preferences to configure automatically the user's privacy settings. The wizard takes into consideration the profile information and connections. Bilogrevic et al. [115] presented an information-sharing system called SPISM. Using machine learning techniques and user's behavior, the system predicts the level of detail for each sharing decision and decides what information to share and at what granularity. Cheng et al. [116] proposed a user-to-user relationship-based access control (UURAC) model for OSNs. The model allows users to express more fine-grained access control policies in terms of the depth of relationships in the network.
  The challenge of such solutions is basically the tendency of users to ignore the privacy settings and blindly trust the default privacy configurations offered by the OSN systems. To reach the desired potential to protect the privacy of users, privacy settings should be coupled with users awareness and change of behavior.

- **User awareness and change of behavior.** One of the countermeasures to protect the privacy in OSNs against users-related threats is enhancing user awareness of the privacy issues and the necessity of the user engagement with services providers to assure the protection of data against breaches and disclosure. MOSN providers must clarify the purposes for processing data and how it is handled in the system. In addition, they need to display the security information of the platform and disclose the potential threats present in the system. At the same time, the user must pay more attention to the privacy policies and "terms and conditions" provided by the system, before registering in the platform and also whenever a change occurs. Once registered, the users are required to change the default visibility and privacy settings before any publication. Furthermore, the users are responsible for any publication of sensitive information about themselves or others, and they must be very careful about the friend requests.

2.4 Privacy Metrics in Information Systems

Privacy metrics measure the level of privacy protection provided in an information system. They contribute to decision making and to privacy assessment and evaluation. A privacy metric uses the properties and functionalities of a system as an input and generates a numerical value that allows to evaluate the privacy level in the system and subsequently to compare different systems.

2.4.1 What are Metrics?

Understanding privacy assessment and evaluation of a system starts with a definition of what a metric is. The Oxford dictionary defines a metric as "a system or standard of measurement" [117]. They are defined as well as "tools designed to facilitate decision making and to improve performance and accountability through collection, analysis, and reporting of relevant performance-related data" [118].

Metric and measurements are similar enough that the two terms are commonly used interchangeably. However, there is a difference between the two terms: measurements provide single-point-in-time views of specific factors while metrics provide standardized procedures and calculation methods to generate relevant numbers of the measured system [119]. In other words, measurements result from observations, while metrics are abstract and they represent the observed data in kind of scale in order to compare and analyze the results [120, 121].

2.4.2 What Constitutes "Good" Metrics?

Different characteristics have been proposed to assist in the development, selection, and implementation of ideal metrics and measures to be used in the information system. Some proposed factors to be considered for a good metric include:

- Quantifiable measures, readily obtainable data, repeatable information processes, and useful measures for tracking performance and taking decisions [122].
- SMART, that is Specific, Measurable, Attainable, Repeatable, and Time-dependent [119].

- Meaningful, reproducible, objective and unbiased, and able to measure progress towards a goal [123].
- Consistently measured, cheap to gather, expressed as a cardinal number or percentage, and contextually specific[124].
- Ease of data collection, relevant indicators, ease of interpretation, and evidence as to the measure's fitness for a purpose need [125].

2.4.3 Metric Life cycle

The life cycle of a metric adopts the following 3C process [120, 121]:

1. Create: gather input data about the investigated system from different providers and sources.
2. Compute: apply a series of operations on the gathered data to derive quantifiable results.
3. Communicate: communicate and disseminate the metric results to the concerned people.

2.4.4 Privacy Metrics in MOSNs

Recently, the number of privacy and data breaches has increased with massive leakage of information. For example, in 2016 the professional social network LinkedIn was hacked and around 167 million credentials were compromised and sold in the dark web marketplace [126]. In this regard, the users of MOSNs are still incapable of evaluating the privacy risk existed when using the services of MOSNs. Therefore, there is a need of formal metrics to quantify the privacy and evaluate the performance and the efficiency of the privacy-preserving techniques implemented in MOSNs.

The mathematician William Thomson stated that "to measure is to know," and "if you cannot measure it, you cannot improve it." Measuring and evaluating the efficiency and effectiveness of the implemented techniques help to identify the flaws and to improve the system in question. Privacy metrics can be used for decision making and in assessing, monitoring and predicting potential privacy threats in the system. Privacy measurements offer the opportunity to make informed decisions about the design of systems, the selection of controls, and the efficiency of the implemented privacy techniques. Furthermore, evaluation of privacy empowers the community with a strong understanding of privacy and better protection of information in the MOSNs.

With the emergence of new systems and networks that advocate for privacy protection, a need of a standardized model to quantify the effectiveness of private networks has appeared. However, measuring and evaluating the privacy is challenging since privacy itself is subjective and it is not easy to define.

In principle, when talking about privacy protection in MOSNs, two different approaches emerge:

1. Those who attempt to protect the user's identity. Privacy is achieved by implementing techniques to hide the identity of the users and the relationship between the users.

2. Those who focus on protecting user's data. To evaluate the effectiveness of such approach, the privacy level of MOSNs is measured to indicate the risk implications of the daily social network activities on the privacy of the users.

In the following, we investigate the different works proposed in the literature for the two approaches.

Anonymity Scores in OSNs

Researchers have focused on quantifying the anonymity of private networks. The following describes some examples of anonymity metrics that have been proposed over the years:

- **Crowds-based metric** was initially developed for Crowds network, but it has been used later to quantify other networks. Reiter et al. [127] have proposed to use the probability p assigned by an attacker to an anonymous sender and they have come up with an anonymity degree as $d = 1 - p$. The metric considers each user separately.

- **Anonymity set size** was proposed by Berthold et al. [128]. It was defined as the size of possible senders in a communication. This metric depends only on the number of users in a system. The degree of anonymity is calculated as $d = \log_2 n$ where n is the number of users of the system.

- **Shannon-Entropy-based metrics**: Serjantov et al. [129] and Díaz et al. [130, 131] proposed two similar anonymity metrics. They used Shannon's theories on entropy to measure the effective anonymity set size. They defined this latter as the uncertainty H (P) regarding which user sent a message:

  $$H(P) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

  where p_i is the probability assigned by an attacker to the subject i, in the anonymity set, linked to the item of interest. In this case, $0 \leqslant H(P) \leqslant log_2 n$, where is the maximum entropy of the system to measure and n is the size of the anonymity set. However, Díaz et al. [130, 131] proposed to normalize the previous equation and get a degree of anonymity that quantifies the performance of the system on a scale from 0 to 1.

  $$d = \frac{H(P)}{\log_2 n}.$$

  Both the metrics can be computed from each other, however, the effective anonymity set size is tied to the size of the anonymity set while the degree of anonymity focuses on the performance of the system. The metrics also are related to the probability of the attackers and they quantify the anonymity with respect to a specific attack. Any change in the attack model induces changes in the obtained results.

- **Other entropy-based anonymity metrics** have been proposed in the literature, like:

  – Local anonymity measure using min and max entropy proposed by Tóth et al. in [132]. They argued that the attacker is successful to disclose the

identity of a user if s/he can compromise the message with a probability than a certain threshold, unlike the previous metrics that quantify the number of bits required to perfectly trace the message to its sender. Θ is defined as the maximum probability assigned to any user of being the sender of the message: $\Theta = max(P)$ where Θ varies between $\frac{1}{n}$ and 1.

- As a generalization of the previous metrics (Shannon-entropy qnd Min-Max entropy), Claußet al. [133] proposed to use Rényi entropy to measure the uncertainty of the identity of an entity, from the attacker's point of view.

$$H_\alpha(P) = -\frac{1}{1-\alpha}\log_2 \sum_{i=1}^{n} p_i^\alpha$$

- scaled anonymity set size was proposed by Andersson and Lundin [134]. It's an entropy-based metric A based on the effective anonymity set size proposed in [129]and in [130, 131].

$$A = 2^{H(P)}$$

- **Other anonymity metrics:** some other works in the literature have proposed to use possibilistic instead of probabilistic methods like described in [135, 136].

Beach et al. [137] have evaluated the well-known anonymity models, such as k-anonymity [99] and t-closeness [138], in case of OSNs and they have deduce that they cannot be applied to the most common form of private data released in social networks. As a solution, the authors proposed an alternative anonymity model called q-Anon. This new model measures the probability that an attacker may use in a query response to map the private data released to a user. Another metric was proposed by Kamiyama et al. [139] to measure the degree of information leakage caused by posting in social networks. They used join entropy to measure the uncertainty about related events (X, Y)

$$H(X,Y) = -\sum_x \sum_y p(x,y)\log_2 p(x,y)$$

and the conditional entropy to quantify the uncertainty X of an event given an information Y.

$$H(Y|X) = -\sum p(x)\sum p(y|x)\log p(y|x)$$

Puglisi et al. [140] have proposed an approach to measure the anonymity risk induced from posting new contents or new activities. They used Kullback–Leibler(KL) divergence [141] between the user profile p and the interests of the overall population q.

$$D(p||q) = \sum_{i=1}^{n} p_i \log \frac{p_i}{q_i}$$

Where 1,..,n is the set of predefined categories of interests.

Privacy Scores in OSNs

With the great success and spread of OSNs, there has been increasing research interest in mechanisms and methods that advocate for privacy protection. Many research studies have been performed on privacy preservation in OSNs by integrating new privacy protection mechanisms in already existing social networks functionalities or by proposing new built-in privacy systems. The increasing number of solutions and

systems that aim to protect privacy in OSNs has led to the necessity to evaluate the efficiency and effectiveness of privacy protections mechanisms proposed.

One of the first attempts in the existing research on privacy metrics was proposed by Maximilien et al.[142] in 2009. The authors proposed a framework to calculate the privacy score based on the sensitivity β_i and the visibility $V(i,j)$ of profile items $i \in i, ..., n$ for of user j in a social network.

$$PR(i) = \sum_i PR(i,j) = \sum_i \beta_i * V(i,j)$$

They have conducted a survey where the questions were designed to determine the privacy degree that users are willing to disclose each information in their profiles. The authors did not offer any dataset to measure the effectiveness of their model.

Liu and Terzi extended the approach in [143]. The authors developed a mathematical model to measure the privacy score of the users in OSNs, based on the sensitivity and the visibility of attributes, using concepts from Item Response Theory (IRT). To evaluate the effectiveness of the score, the authors used both synthetic and real-world datasets. However, the proposed model assumed that the users are independent, the attributes are independent and it did not take into consideration the inferred data. Srivastava and Geethakumari extended Liu et al.'s model and included the hidden data in [144]. They introduced also privacy leakage to quantify the privacy exposure for some user from a message. The score was calculated by dividing the sensitivity for the message by the sum of sensitivities over all messages. Both models [143] and [144] assumed that the sensitivity and visibility are the same across all users.

Petkos et al. [145] enhanced the previous models and proposed a PScore framework. It considered the user's personal preferences in scoring the attributes, it included the hidden and inferred information and it was structured based on different types of information. Pensa and Di Blasi introduced a new privacy assessment framework in [146] to measure the privacy leakage and set a model of privacy preferences for each user. The framework calculated the privacy score from the privacy matrix computed from the user's preferences. If the score exceeded a given threshold, the framework would notify the user about the privacy risk. The privacy score was based on both the sensibility and the visibility of user profile attributes. This work was inspired from the model proposed by Liu and Terzi [143], but it took into consideration the circle (friends) of the users where the willingness ratio of a user to disclose information is proportional to the number of her or his friends.

Bonneau and Preibusch [147] evaluated the privacy settings and policies of 45 social networks using privacy and functionalities score. The privacy score was an arithmetic mean of 3 subscores:

- Data collection subscore was calculated from the number of data collected at a site.
- Privacy control subscore was calculated based on the number of privacy control features in an OSN.
- Privacy policy subscore was based on the availability of policy and its accessibility.

Other research evaluated privacy from another aspect other than the sensitivity and visibility. Becker et al. [148] introduced PrivAware. The tool quantified the privacy risk from the amount of information inferred in social networks. The privacy

score was calculated as the total of visible attributes divided by the total of attributes in a profile. PrivAware mapped the privacy risk to a grading score and set recommended actions for users. Ngoc et al. [149] presented a privacy metric calculated based on probability and entropy theory. This metric quantified the information leaked in the users' posts. The authors built the metric based on the idea of how much an attacker can reveal hidden sensitive information of a user from the sentences in the posts. Talukder et al. [150] proposed Privometer to measure the leakage of sensitive information based on the profiles of users and their social graphs. The privacy score was the combined probability of sensitive attribute inference from the information on the friends' profiles. Privometer ranked the relationships of users based on the amount of information leakage and suggested self-sanitization recommendations to control the leakage. Akcora et al. in [151] suggested measuring the risk score based on the feedback of users about others in OSNs and the sensitive information disclosure. The framework computed the risk level in terms of friends attitude and the similarities with the users. The authors adopted an active learning process where a classifier was built on the user's risk labels and was used to predict the risk labels of other strangers. The authors used Facebook and real datasets to evaluate the effectiveness of the model. Similar to this metric, Vidyalakshmi et al. [152] proposed a privacy scoring framework based on the output of friends, their ranking and the total number of friends. The framework helped the users assess the information sharing behavior and in taking a decision of who can see what information.

Nepali and Wang [153] presented a real-time model to calculate the privacy risk indicator (PIDX) based on the sensitivity and the visibility of attributes. SONET was based on 2 components, attribute to attribute (actor model) and user to user relationships (community model). SONET included hidden information that is not firsthand available, but they infer from direct data. The model was used to monitor the level of privacy in OSNs and to protect users from sensitive information disclosure. The authors extended the actor model of SONET in [154] and the community model in [155]. They included 3 metrics: known attribute list (direct, hidden and virtual), attribute sensitivity and attribute visibility. They proposed three privacy measurement functions:

- Weighted privacy index: w-PIDX to measure an entity's privacy based on the attribute list weight, and w-PIDX (i,j) to measure the privacy exposure between two actors.
- Maximum privacy index: m-PIDX measures an entity's privacy based on the maximum attribute impact factor of all known attributes, and m-PIDX (i,j) measures the maximum privacy exposure.
- Composite privacy index: c-PIDX combines both privacy indexes.

The authors introduced the OSNPIDX tool in [155] as an implementation of SONET model. OSNPIDX defines an actor with 20 static-assigned privacy impact factor attributes.

Table 2.2 summarizes briefly the reviewed privacy scoring approaches.

2.5 Summary

This chapter has introduced the concepts of Microblogging Online Social Networks, privacy in the context of OSNs, and privacy metrics for the purpose of setting up the necessary knowledge for the rest of the present thesis.

TABLE 2.2: Overview of the reviewed privacy scoring approaches

Privacy score	**Description**	**Features**
Privacy Scores: [142, 143, 144, 145, 146]	A score generated based on the sensitivity and visibility of the items posted by an OSN user. Some scoring frameworks take into consideration the hidden and inferred information and the social graph.	Profile items, sensitivity per item, visibility per item. For some metrics, leakage per item is also included.
PrivAware: [148]	The score is calculated based on the total of visible attributes divided by the total of attributes in a profile.	The amount of information inferred in social networks.
Privometer: [150]	A score generated based on the sensitivity of the profiles of users and their social graphs.	Sensitive attribute inference from the information available in immediate friends' profiles.
Privacy score from social graphs: [151], [152]	A score calculated based on the risk level in terms of the friends attitude and the similarities with the users.	How much an attacker can reveal of relationships.
Privacy Index: [153, 154, 155]	A real time score calculated based on the sensitivity and the visibility of public attributes.	Sensitivity score per item, visibility level per item.

First, we discussed Microblogging Online Social Networks, their stakeholders and the different types of data used. Then, we tried to define privacy and we reviewed the current state-of-the-art in privacy laws and privacy requirements. Furthermore, we have explored the concept of privacy in the context of MOSN, we discussed the privacy threats and attacks that OSNs suffer from and we examined the techniques and the countermeasures that address these privacy issues. Additionally, we explained the importance of evaluating and quantifying privacy in MOSNs and we presented studies related to the present research dealing with evaluation, measuring, and computing privacy scores in the context of OSNs.

This chapter has shown that MOSNs offer various functionalities and services that attract a great number of users to online social services. The public interest in privacy protection has increased due to the growing amount of data breaches of common and extended use services, especially that many users jeopardize their private life by sharing sensitive information. In this regard, users are still incapable of evaluating the privacy level when using the services of OSNs.

The existing literature discussed in this chapter reveals that all the privacy models evaluate the privacy in OSNs from the user's perspective. They assessed privacy based on the visibility and the sensitivity of the attributes from a user's profile, such as name, age, address, phone number, etc. However, systems vary regarding the attributes they require users to provide, hence the usage of attributes limits the evaluation of privacy in OSNs. Furthermore, the models considered the impact of the visibility of attributes to other users but not to the system provider. They did not include other aspects of privacy protection, for example, how the storage type can affect the privacy of the data. Another limitation of the previous models is that they did not consider security requirements in their evaluation, however, privacy and security concepts should not be separated since they are intertwined. Furthermore, the previous privacy metrics use system-specific measurements, thus it is difficult to compare privacy scores across systems.

Therefore, there is a need of a generic framework that quantifies the privacy level provided in the systems and can be used to compare between different systems. To respond to this need, the present thesis proposes a novel generic framework to measure and assess the privacy level of MOSNs.

In the following chapters, an analysis of the sharing behavior of users in OSNs and their preferences will be discussed in Chapter 3. Then, Chapter 4 will present a qualitative comparative study of different microblogging OSNs in terms of privacy and security characteristics. Further, an algorithmic model to evaluate and assess privacy in MOSNs will be defined in Chapter 5. Finally, the microblogging systems of Chapter 4 are evaluated in 6 using the privacy scores obtained from the proposed privacy metric in Chapter 5.

Chapter 3

Privacy and Information Sharing in Microblogging OSNs

When it comes to privacy in OSNs, the users live in a privacy paradox ([156]), worried about protecting their privacy and at the same time accepting to share data as a price for enhancing their digital presence ([157]). They have the continuous fear of what happens to their private information once it is released ([19]), however, they voluntarily join OSNs and disclose large amounts of personal information ([158]).

Various studies have investigated the privacy paradox between the expressed privacy concerns and information sharing in OSNs. For example, the results of the analysis from Lutz and Strathoff's study ([159]) showed that privacy paradox can be confirmed in the case of users of institutional services (e.g. banks and government), whereas users of online social networks are more vigilant to their data. Studies ([160, 161, 162, 163]) proved that indeed privacy concerns are related to information revelation practices and individuals who are concerned more about their privacy are more aware of their online interaction than the less concerned individuals. However, other studies ([164, 165, 166]) showed that there is no relationship between perceived privacy awareness and information sharing behavior.

In light of the previous discussion, we analyze, in this chapter, two following research questions:

- RQ1: What are the factors that influence information sharing behavior in OSNs?
- RQ2: What are the users' preferences in terms of privacy in OSNs?

To answer these questions, throughout this chapter, we examine the results of a statistical analysis of 542 participants from different age groups: Section 3.1 explains the followed research methodology, it outlines the methods and procedures used to develop the questionnaire and to analyze the results. Section 3.2 answers the first research question and presents the findings of the study, while Section 3.3 discusses the results of the study that answer the second research question. Section 3.4 concludes the current study.

3.1 Data Gathering Methodology

To answer the research questions, the study began by designing and conducting an online questionnaire survey using Google Forms [1].

[1] https://www.google.com/forms/about

3.1.1 Methodology

The questionnaire survey had 28 questions intended for Online Social Networks' users (refer to appendix A), where the first question was a filter that asked the users if they were using OSNs and 3 questions were socio-demographic questions asking about participants' age, gender, and education. The survey was not specific to one system but based on the most used OSN by the participants. In this study, the population refers to students of Open University of Catalunya (UOC) [1]. The survey was available in three languages: Catalan, Spanish, and English, and distributed via university students' email accounts.

To maximize the response rate, the survey was sent to 4200 participants using the Data Science Lab initiative of Internet Interdisciplinary Institute (IN3)[2] from Universitat Oberta de Catalunya (UOC) located in Barcelona, Spain.

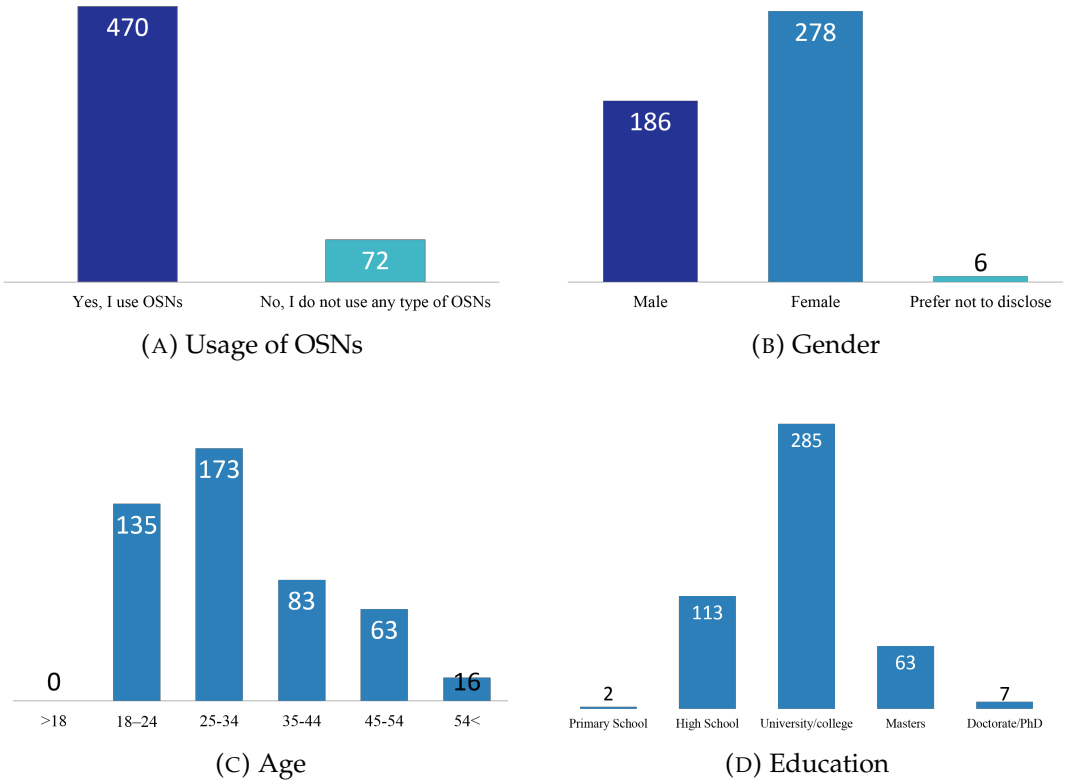
The participation was voluntary and anonymous. The participants were selected randomly and gender balanced. They were informed of the purpose, the objectives, and the duration of the project. Their consent was obtained before starting collecting the data. The survey was available online for one month (April 2018). It yielded to 542 usable responses after excluding incomplete responses.

3.1.2 Summary of Descriptive Analysis

Out of the 542 respondents who answered the survey questionnaire, 72 participants (13%) did not use any type of OSNs for various reasons (privacy concerns, OSN are useless, waste of time, social stress, misinformation and misleading, misuse of information by third parties, OSNs break human relationships...), while 470 participants (87%) confirmed that they were daily using OSNs. Fig. 3.1 presents some statistics describing the participants.

Of the 470 participants who confirmed that they were using at least one type of OSNs, 59.15 % of the participants were female, 39.57 % were male, and 1.28 % preferred not to reveal their gender. 50% of the participants were between 18 and 34 years. Most of the participants had already or were at that time preparing for a university degree (60.64 %). Table 3.1 shows the demographics of the data collected.

[1] http://www.uoc.edu/portal/en/index.html
[2] http://www.uoc.edu/portal/en/in3/index.html



(A) Usage of OSNs (B) Gender

(C) Age (D) Education

FIGURE 3.1: Demographic data of participants

TABLE 3.1: Profile of Participants

Profile	Items	Freq.	Percentage
Gender	Female	278	59.15 %
	Male	186	39.57 %
	Prefer not to disclose	6	1.28 %
Age	$<$ 18 years	0	0%
	18−24 years	135	28.72 %
	25−34 years	173	36.81 %
	35−44 years	83	17.66 %
	45−54 years	63	13.40 %
	$>$ 54 years	16	3.40 %
Education	Primary School	2	0.43 %
	High School	113	24.04 %
	University/college	285	60.64 %
	Masters	63	13.40 %
	Doctorate/PhD	7	1.49 %

3.2 What Influences Information Sharing Behavior in OSNs?

Given the number of privacy concerns in OSNs, several models have been analyzed to understand the relationship between privacy concerns and information sharing behavior in OSNs. The previous studies focus on analyzing the relationship between the sharing behavior and one or two dimensions of privacy concerns. There is a

considerable lack of studies that cover the relationship between all aspects that can have an effect on information sharing behavior in OSNs.

3.2.1 Theoretical Framework

In this study, we provide an overall analysis of the factors that influence the information sharing behavior of users in OSNs. We analyze 8 factors, namely: (1) information sharing behavior, (2) perceived privacy awareness,(3) perceived control of information, (4) data collection limitation, (5) policies understanding, (6) privacy functionalities and granularity, (7) age, and (8) gender. The perceived privacy awareness, perceived control of information, and data collection limitation factors are based on the Internet User's Information Privacy Concerns (IUIPC) model ([167]) while the other factors are derived previous studies (e.g. [162, 168, 169]).

The IUIPC model consists of three dimensions: (1) awareness refers to the awareness of users about privacy issues and practices in data-handling companies, (2) control refers to the right to determine how the information is processed (collected, stored, and sold), and (3) data collection is the extent to which a person is concerned about the amount of data possessed by others. We detail each of these factors in the following:

1. **Information Sharing Behavior (ISB)**

   Information sharing behavior describes the behavior of users towards revealing information about themselves. The business model of OSNs revolves around the sharing of personal information of users. A great number of users have open profiles and they reveal sensitive information to others. In May 2018, a study on cyber-security and trust in Spanish households found out that 34.1% of social network users reveal their published data to third parties and/or everyone on the Internet and 5.5% of the users declare that they do not know the privacy level of their profile ([170]).

2. **Perceived Privacy Awareness (PPA)**

   Perceived privacy awareness refers to the perception of the users of privacy in OSNs. It measures the level of users' awareness of the present privacy threats in OSNS. OSNs' users are concerned about the threats that social networks present in terms of privacy breaches. Yet, they behave differently to protect their privacy.

3. **Perceived Control of Information (PCI)**

   Perceived control of information analyzes the attitude of users towards the importance of controlling the access to information. According to traditional theories ([171, 172]), individuals create imaginary boundaries and barriers to protect their information. For example, in face-to-face situations, people tend to whisper or tell just a group of friends a piece of private information. Similarly, the users of the virtual world require techniques and mechanisms to control access to their information ([173]).

4. **Data Collection Limitation (DCL)**

   Data collection limitation refers to the understanding of the importance of limiting data collections in OSNs. Privacy laws and regulations state that the information stored must be limited to what is necessary to operate (refer to

section 2.2.1). The amount of information collected from OSNs on each individual can be analyzed and processed to provide a complete picture of the user. Although the OSNs are required to protect the data by anonymizing them, the anonymization techniques are far from sufficient to protect privacy. Anonymized datasets are still at risk because correlating the data from different sets can leak information ([174]). Narayanan and Shmatikov ([96]) have shown that a person can be easily identified in an anonymous graph of Twitter using another OSN as a source of auxiliary information.

5. **Policies Understanding (PU)**

   Policies understanding is related to how much the users understand the privacy policies provided by OSNs. OSNs come under criticism for the ambiguity of their privacy policies. They are expressed in vague terms and in technical jargon, which makes these policies difficult to understand ([175]).

6. **Privacy Functionalities and Granularity (PFG)**

   Privacy functionalities and granularity refer to the perception of users about the importance of granular privacy settings as a mechanism for privacy protection. Privacy settings vary from one social network to another and there is no standard for controlling personal information. To protect their data, users have two ways. The first one is to refrain from sharing information in OSNs, but this is not practical, giving that the main purpose of OSNs is to share information and communicate with others. The second option is to use the privacy settings provided by the OSNs. But these mechanisms remain insufficient and not flexible to protect the users ([176, 177]).

3.2.2 Research Hypothesis

To answer the research questions and based on the above discussion, we formulated the following hypotheses:

- **H1**: Privacy awareness influences positively the behavior of information sharing.
- **H2**: Information control influences positively the information sharing behavior.
- **H3**: The understanding of the importance of data collection limitation influences positively the information sharing behavior
- **H4**: Privacy policies understanding influences positively the information sharing behavior.
- **H5** : Privacy settings granularity influences positively the information sharing behavior.
- **H6** : Age influences positively the information sharing behavior.
- **H7** : Women and men behave the same way when it comes to sharing their information in OSNs.
- **H8** : Users tend to behave differently when sharing information with friends and contacts (on their own timeline) than when sharing with other users (in groups).

3.2.3 Reliability Analysis and Items Validity

To evaluate the internal consistency of the items, a Cronbach alpha reliability test ([178]) is conducted. The output of the analysis is considered acceptable if the Cronbach's alpha value is above 0.70 ([179, 180, 181]). The higher the score, the more reliable the factor is.

To conform with other studies in the same area, for all tests, a p value < 0.05 is considered statistically significant ([161, 160, 182]). In this study, the higher scores indicate a greater level of understanding of the factor.

The results of reliability analysis along with the number of items, the mean and standard deviation values are reported in table 3.2. The results show that all Cronbach's alpha values are above the acceptable threshold, therefore, we can conclude that all factors have adequate internal consistency and are suitable for the study.

TABLE 3.2: Reliability Analysis - Cronbach's alpha Values

Factor	**Nº items**	**Cronbach's α**	**Mean**	**SD**
Information sharing behavior (ISB)	3	0.948	3.543	0.726
Perceived privacy awareness (PPA)	2	0.740	4.171	0.480
Perceived control of information (PCI)	7	0.775	3.734	0.452
Data collection limitation (DCL)	3	0.817	4.149	0.572
Policies understanding (PU)	3	0.771	2.584	1.067
Privacy functionalities and granularity (PFG)	4	0.852	3.602	0.531

Note: SD refers to standard deviation.

3.2.4 Analysis Results

To validate the hypothesis, we conducted different statistical analyses as follows:

- **Correlation and regression**

  To analyze the influence of privacy awareness (H1), information control (H2), data collection limitation (H3), privacy policies understanding (H4), privacy settings and functionalities (H5), and age (H6) on information sharing behavior, Pearson correlation ([183]) and multiple linear regression ([184]) were performed. Table 3.3 reflects the results of Pearson correlation analysis. Table 3.4 represents the results of multiple regression analysis.

  The results in table 3.3 show that information sharing behavior is significantly predicted by privacy awareness, perceived control of information, data collection limitation, and privacy functionalities granularity. The results were confirmed by multiple ultiple regression analysis, as shown in table 3.4. These variables statistically significantly predicted information sharing behavior, F(4, 465) = 80.37, p value < 0.000, R^2=0.409, with data collection limitation showing a greater influence. The overall model explains 40.9% of the variance in information sharing behavior. The results show that age and privacy policies understanding do not influence information sharing behavior (p value > 0.05).

TABLE 3.3: Correlation Matrix

		ISB	**PPA**	**PCI**	**DCL**	**PU**	**PFG**	**Age**
	Corr. Coeff	1						
ISB	*p* value							
	Corr. Coeff	**0.248(*)**	1					
PPA	*p* value	**5.25e-08**						
	Corr. Coeff	**0.465(*)**	**0.284(*)**	1				
PCI	*p* value	**<2.2e-16**	**3.67e-10**					
	Corr. Coeff	**0.569(*)**	**0.146(*)**	**0.498(*)**	1			
DCL	*p* value	**<2.2e-16**	**0.002**	**<2.2e-16**				
	Corr. Coeff	0.049	0.009	**0.157(*)**	**0.149(*)**	1		
PU	*p* value	0.288	0.838	**0.0006**	**0.001**			
	Corr. Coeff	**0.407(*)**	0.009	**0.349(*)**	**0.417(*)**	0.018	1	
PFG	*p* value	**<2.2e-16**	0.851	**5.87e-15**	**<2.2e-16**	0.702		
	Corr. Coeff	0.085	-0.036	0.027	0.031	**0.249(*)**	0.030	1
Age	*p* value	0.065	0.436	0.566	0.500	**4.49e-08**	0.515	

(*) Correlation is considered significant at $p < 0.05$

Note: ISB: Information sharing behavior; PPA: Perceived privacy awareness; PCI: Perceived control of information; DCL: Data collection limitation; PU: Policies Understanding; PFG: Privacy functionalities and granularity.

TABLE 3.4: Multiple Linear Regression Results

	B	**Std. Error**	β	**t**	***p* value**
Constant	-1.313	0.308		-4.260	0.000
PPA	0.215	0.057	0.142	3.798	0.000
PCI	0.268	0.070	0.167	3.859	0.000
DCL	0.492	0.055	0.387	8.975	0.000
PFG	0.255	0.055	0.186	4.642	0.000
R^2=0.409, F(4,465)=80.37, $p < 0.000$					

- **Gender influence on information sharing behavior**

  To analyze the 7th hypothesis (H7) of our model, a T-test analysis ([185]) was conducted to compare the difference between the gender concerning their behavior towards information sharing in OSNs. The analysis considers only two genders (female and male) and ignored the data from the participants who preferred to not disclose their gender since they were not statistically representative, only 1.3% of the sample (see table 3.1). The sample size of the study is 464 (female= 278, male=186). The assumption of homogeneity of variance is satisfied via Levene's F test, F=1.146, p=0.285 for information sharing behavior and F=1.415, p=0.235 for privacy awareness.

  Table 3.5 shows that there is a difference between women (M=3.528 (SD=0.729)) and men (M=3.557(SD=0.717)) in their perception of privacy threats, t(462)=2.107, p=0.036. Women are more aware of privacy threats in OSNs than men. Furthermore, the results show that there is no significant difference between the women (M=4.209 (SD=0.438)) and men (M=4.113 (SD=0.537)) when it comes to the way how they share information in OSNs t(462)=-0.426, p=0.670.

TABLE 3.5: T-test Analysis: Gender Comparison

	Levene's Test		**t-test for Equality of Means**							
	F	*p* value	t	*p* value	Female		Male		Mean Diff	SD Diff
					Mean	SD	Mean	SD		
ISB	1.146	0.285	-0.426	0.670	3.528	0.729	3.557	0.717	-0.029	0.069
PPA	1.415	0.235	2.107	**0.036** (*)	4.209	0.438	4.113	0.537	0.096	0.045

(*) significant at $p < 0.05$

Note 1: SD refers to standard deviation.

Note 2: ISB: Information sharing behavior; PPA: Perceived privacy awareness.

- **Group behavior vs individual behavior**

  To answer the 8th hypothesis (H8), the study examined the behavior of participants in terms of sharing information with their friends and contacts versus the information sharing behavior when the participants share the information with other users of the OSNS (they are part of the same group of interests but they are not acquainted). The results (see table 3.6) show that the sharing behavior with friends and the sharing behavior in groups (with strangers) is statistically associated. The participants behave in the same way when it comes to sharing with friends as in sharing in groups of strangers. In other words, the participants who tend to share more (or less) information with their friends behave in the same way when it comes to sharing in groups with strangers.

TABLE 3.6: Sharing in Groups vs Sharing Individually

		Sharing Individually	**Sharing in Groups**
Sharing Individually	Corr. Coeff	1	**0.8560** (*)
	p value		**<2.2e-16**
Sharing in Groups	Corr. Coeff		1
	p value		

(*) Correlation is considered significant at $p < 0.05$

3.2.5 Hypothesis Results and Discussion

The results of the analysis showed that the users who are aware of privacy concerns in OSNs tend to share less information about themselves (**H1 supported**). This is in line with previous studies ([160, 161, 162, 163]) that revealed that privacy concerns are proportionate with information revelation practices and individuals who are concerned more about their privacy are more aware of their online interaction than the less concerned individuals. The result is also in line with Rogers's protection motivation theory ([186]) that argues that understanding risks motivates a protection behavior. In this study, there is no privacy paradox to report.

Furthermore, the information sharing behavior is influenced by the perceived information control (**H2 supported**), by the importance of data collection limitation (**H3 supported**), and by the granularity of privacy functionalities and settings (**H5 supported**). This is again in line with Rogers's theory ([186]). The users that are inclined to protect their privacy tend to share less information. However, it is found that understanding privacy policies do not report a significant influence on information sharing behavior (**H4 rejected**). This can be explained that privacy policies can govern the data collection and prevent abuse of personal data, but they fail to prevent privacy threats that emerge from a social environment like cyber-bullying.

In addition, the analysis revealed that age does not have an influence on the way users share their information (**H6 rejected**). The result was confirmed by previous studies ([161, 168] where age does not make a difference in the behavior in OSNs, while [187, 188, 189]) showed that younger users are more engaged in sharing information than older users due to the desire of popularity and impression ([157]).

Even though the gender factor was fully analyzed in previous studies ([169]), it was included in the study for a more complete analysis. The results confirmed that women and men are different when it comes to their perception of privacy threats. However, there are no significant differences between men and women regarding their information sharing behavior (**H7 supported**).

Furthermore, and contrary to our expectations, the results showed that there is no difference of information sharing behavior of users with strangers or with friends and contacts, they behave the same way when participating in groups of strangers or when they share information with their friends (**H8 rejected**). Again, this is in line with Rogers's theory ([186]), that once an individual is aware of the privacy risks, they tend to change their behavior, either in a trusted environment or with strangers.

In addition to the results of the hypothesis, the analysis of the survey questionnaire has shown existing relationships between different factors. Our findings include: Privacy awareness is influenced by perceived control of information and data collection limitation, perceived control of information can be influenced by data collection limitation, understanding privacy policies, and granularity of privacy functionalities, while the data collection limitation can be influenced by understanding privacy policies and granularity of privacy functionalities. Table 3.7 summarizes the findings.

TABLE 3.7: Relationship Between Factors

	ISB	**PPA**	**PCI**	**DCL**	**PU**
Perceived privacy awareness (PPA)	✓				
Perceived control of information (PCI)	✓	✓			
Data collection limitation (DCL)	✓	✓	✓		
Policies understanding (PU)			✓	✓	
Privacy functionalities and granularity (PFG)	✓		✓	✓	

Note: ISB: Information sharing behavior.

3.3 What Are the Users Preferences in Terms of Privacy in OSNs?

As defined in the introduction 1, Online Social Networks offer users (person or organizations) multiple functionalities to represent their own person in form of a profile and to keep in touch with other users (family, friends, acquaintances, colleagues, ...). The user profile may include demographic information, personal interests, general information, etc. The OSN system may collect and store a record of connections and interactions of users with others, as well as provide several services (photo and video sharing, direct messaging, games, search for other users, etc.) to attract new users and facilitate interactions between users.

To answer our second research question of how the users perceive OSNs, what are their preferences for an ideal OSN system, and how it should deal with their

data and privacy, we identified 8 basic components of OSNs. We have identified these from the definition of OSNs provided by [5] (refer to introduction 1), also from reviewing existing OSNs, and based on the Internet User's Information Privacy Concerns (IUIPC) model ([167]). Below, we discuss the results obtained for each components:

3.3.1 Users Preferences for Profile Management

Social interactions are viewed as performance in a theater, that they are shaped by the performers, the audience members, and the environment [190]. Individuals tend to present themselves to impress the others, which leads to the decision to reveals certain personal aspects and construct a social identity for a particular audience. Similarly, in OSNs, users create and manage a profile and fill it with personal information.

When the participants of our survey questionnaire were asked about their preferences about creating and managing profiles in OSNs, 60% of the participants preferred to register using their email address and logged in with either real name or pseudonym (76% of the participants) and a strong and unique password (34%), as shown in figure 3.2 (refer to appendix B for more details).

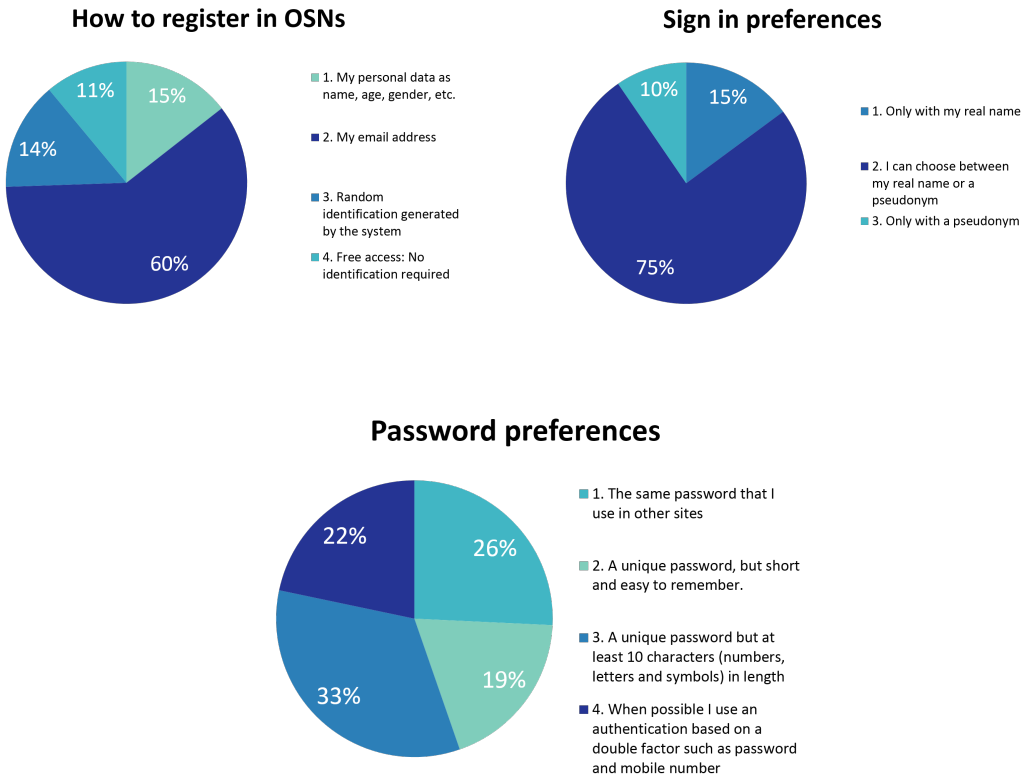


FIGURE 3.2: Profile management preferences

We asked the participants about the items that should be required to create a profile in an OSN and to rank their sensitivity. The results showed that the participants considered username (86%), email address (59%), and first name (51%) the items that should be required and they are not very sensitive. Meanwhile, the participants considered items like surname (69%), Photo (73%), age (75%), gender (77%), social security number (93%), education (93%), phone number (96%), civil status (98%),

postal address (99%), and political (100%) and religion (100%) affiliations should not be required to create a profile in an OSN. They ranked postal address (67%), phone number (73%), and social security number (78%) as very high sensitive items. Tables B.4 and B.5 in appendix B provide details of the answers.

Furthermore, we asked the participants about their preferences of who can access to their profile and see their provided information, most of the participants agreed that they prefer to maintain the access at most to only their friends (those users who they approved of). They preferred that their personal identity information must be maintained private (34%) or at most viewed by only their friends (49%), while they preferred that the access to the profile should be kept accessible to only their friends (69%), as shown in table 3.8.

TABLE 3.8: Profile items visibility

	My identity		**My profile**	
	Freq.	**%**	**Freq.**	**%**
Private	161	34%	51	11%
Friends	230	49%	323	69%
Public to all users of OSN	67	14%	86	18%
Public to Internet	12	3%	10	2%

3.3.2 Users Preferences for Friendship Management

One of the main components defining an OSNs is to create social relationships (e.g. friends, co-workers, acquaintance, etc.). Friendship management combines all functionalities that enable the user of OSNs to connect and communicate with others. Examples for functions enabling friendship management in OSNs are the ability to accept or reject a friendship request and manage the connections list visibility.

In our survey, we asked the participants about the importance of the ability to accept or reject friendship request, to control or limit who can send friendship requests, and the ability to set the visibility of the connections list. The participants agreed that the ability to accept or reject a new contact (55%) and the ability to set the visibility of connections list (53%) are extremely important in an OSN, while the ability to control who can send friendship requests is important (28%) as shown in table 3.9. The participants were asked also about how they preferred the visibility of the connections list in OSNs and 57 % answered as it should accessible only their friends and 34% said that it should not be accessible to anyone, as shown in table 3.10.

TABLE 3.9: Users' preference for friendship management

	Accept / reject requests		**Set visibility to connections list**		**Control friendship requests**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**
Not important	11	2%	22	5%	19	4%
Somewhat important	21	4%	30	6%	48	11 %
Important	70	15%	63	13%	124	28%
Very important	111	24%	107	23%	119	26%
Extremely important	257	55%	248	53%	140	31%

TABLE 3.10: Connection list visibility

	Freq.	**%**
Private	159	34%
Friends	268	57%
Public to all users of OSN	39	8%
Public to Internet	4	1%

3.3.3 Users Preferences for Message Management

OSNs are built to allow users to share their thought and activities. They encourage users to share and improve their digital presence in the virtual world. Information sharing in OSNs can be attributed to different reasons: peer pressure ([191]), personality traits ([192, 193, 194]), trust in the protection provided by the service provider ([192, 194]), etc.

Message management refers to information shared with other users (contacts, OSN providers, the general public, etc.) in the form of messages in the broad sense of the word. Messages include any piece of data that is exchanged between a user and another, like text, interests, photos, and videos. In our study, the participants were asked about their preferences of controlling access to their messages, the sensitivity of their posts, and some message functionalities.

First, the participants were asked about their preference of who can access and read the message they post and who mention them in messages. The participants agreed that only friends and contacts they approved are the ones who should be allowed to access their messages (77%) or mention them (60%). While in the case of mentioning, 29% of the participants preferred that no one should be able to mention them in any message (refer to table 3.11).

Then, the participants were asked to rank the sensitivity of the different topics that can be shared in messages. The participants ranked personal information as very sensitive (26%) to extremely sensitive (50%). They agreed also that religion (43%), politics (45%), health (59%), and personal financial information (61%) are extremely sensitive and should not be shared on the OSNs. While topics like general information, education, work, and business are less sensitive. For more details refer to table B.6 in appendix B.

TABLE 3.11: Post Visibility

	Messages I post		**Who can post about me**	
	Freq.	**%**	**Freq.**	**%**
No one	40	9%	136	29%
Friends	360	77%	280	60%
All users of OSN	61	13%	49	10%
Public (Internet)	9	2%	5	1%

The participants were also asked about the importance of some functionalities to manage messages and posts. They answered that sharing multimedia (e.g. photos and video) is important (34%), while the possibility to edit (39%) and deleting (52%) a published message were extremely important, as shown in table 3.12.

TABLE 3.12: Post Requirements

	Share multimedia		**Rectify Posts**		**Delete Posts**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**
Not important	30	6%	8	2%	12	3%
Somewhat important	84	18%	38	8%	20	4%
Important	162	34%	109	23%	79	17%
Very important	120	26%	131	28%	115	24%
Extremely important	74	16%	184	39%	244	52%

3.3.4 Users Preferences for Group Management

Group in OSNs is a functionality that allows users to interact with other users that share similar interests but not necessarily they figure in their friendship/contact list. Users can create, post, read, and comment to messages posted in the groups. Groups can be open, closed or by invitation-only.

We asked our participants about their preferred method to subscribe to a group and the majority answered that they preferred to subscribe to a group where only the administrator can add users (40%) or the administrator and some chosen users (51%), and where the list of members is visible only to the members (80%), as shown in Fig. 3.3. The participants also preferred that the groups they subscribe to should be by invitation-only (51%) and the messages they post are viewed only by the members of the group (59%), as shown in table 3.13.

Similar to the users' message, the participants were asked to rank the sensitivity of different topics that can be shared in groups. They ranked personal information as extremely sensitive (48%). They agreed also that religion (43%), politics (44%), health (54%), and personal financial information (52%) are extremely sensitive and should not be shared on the groups. while topics like general information, education, work, and business are less sensitive. For more details refer to table B.9 in appendix B.

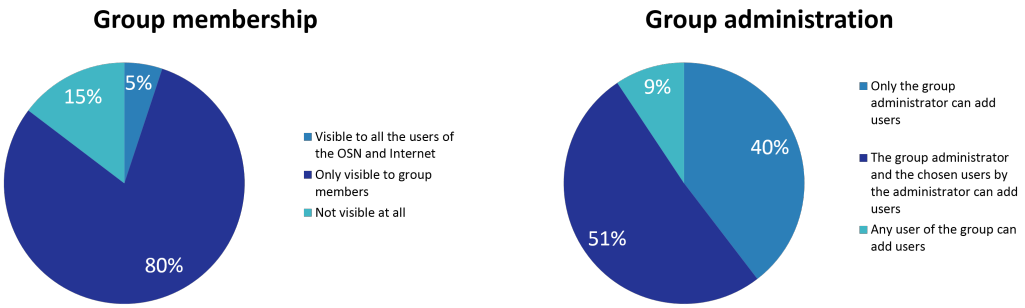


FIGURE 3.3: Group management preferences

TABLE 3.13: Group visibility

	Groups I subscribe to		**My posts in groups**	
	Freq.	**%**	**Freq.**	**%**
Closed	167	36%	136	29%
Members	239	51%	275	59%
Public to all users of OSN	58	12%	49	10%
Public to Internet	6	1%	10	2%

3.3.5 Users Preferences for Privacy Polices

As explained in section 3.2.1, OSNs are criticized for the ambiguity of their privacy policies as they are expressed in vague terms and difficult jargon to understand ([175]). Privacy policies are hidden in the "Terms of Services" which are provided as an external link and ignored most of the time [195]. Furthermore, service providers retain the right to change the clauses of the policies at any time.

The participants were asked if they were informed about the existence of privacy policies in OSNs and 87% confirmed they knew they exist. However, only 6% read the entire document before using the services of OSNs, while 62% read some parts and 32% did not read the documents. Out of 68% of the participants who read the privacy policies (entirely or partially), only 26% understood the clauses of the policies, while 68% understood some parts and 6% did not understand the clauses included in privacy policies.

The participants were asked also if they agreed with the terms and clauses presented in the policies and 26% answered that they agreed because they put trust in OSNs, 57% answered that they do not agree, however, they gave their consent as a price to use the services of OSNs, and 16% answered that if they did not agree with privacy policies, they changed the OSN. Fig. 3.4 presents the results of the users' preferences for the privacy polices.

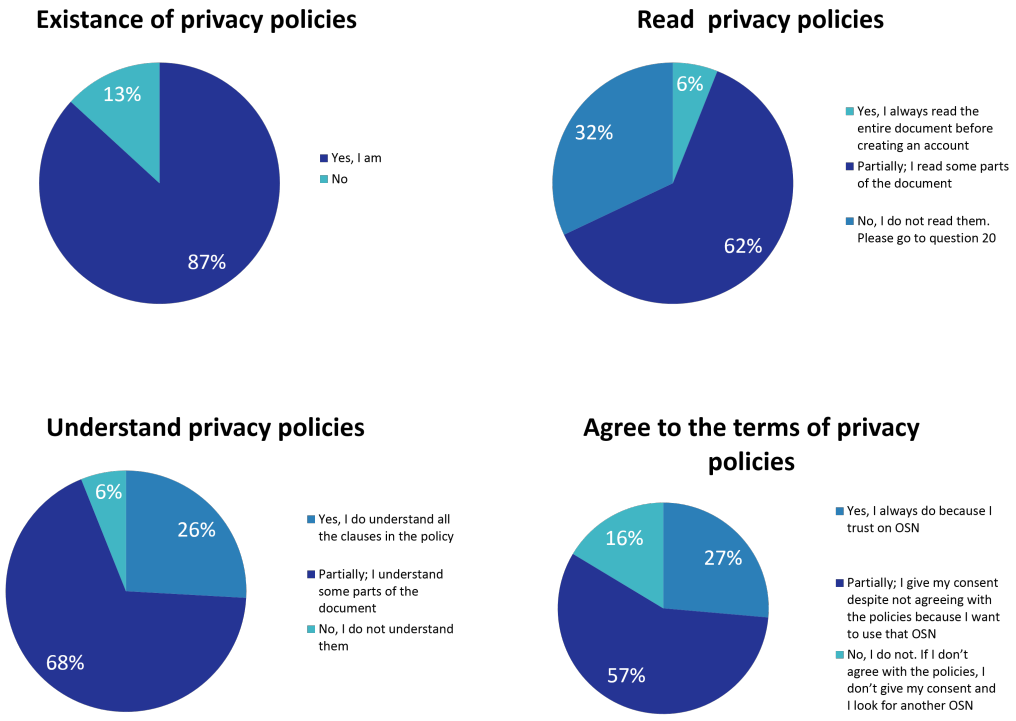


FIGURE 3.4: Privacy polices preferences

3.3.6 Users Preferences for Privacy Settings

As explained in section 2.3.1, unawareness of the existing privacy settings or inadequate configuration of the present privacy settings may lead to disclosing sensitive information to other OSNs users or unregistered users. The participants of our study were asked if the privacy setting presented in the OSNs are easy to use, 40%

confirmed that they were indeed easy to use, 45% found the settings a bit difficult to configure while 15% found them very difficult to use. They were asked as well if privacy settings were enough to protect the privacy of users and data, only 4% confirmed that privacy settings are enough to protect privacy while 68% said that privacy settings should be fine-grained, and 28% said that privacy settings cannot protect users' privacy, as represented in Fig. 3.5 and tables B.10 and B.11 in appendix B.

The participants were asked also to rank the importance of some privacy settings to control the visibility of profile, messages, personal information, and content search. Most of the participants agreed that all these settings are very important if not extremely important to build a privacy-protecting OSNs. Table B.12 in appendix B gives more details about this.

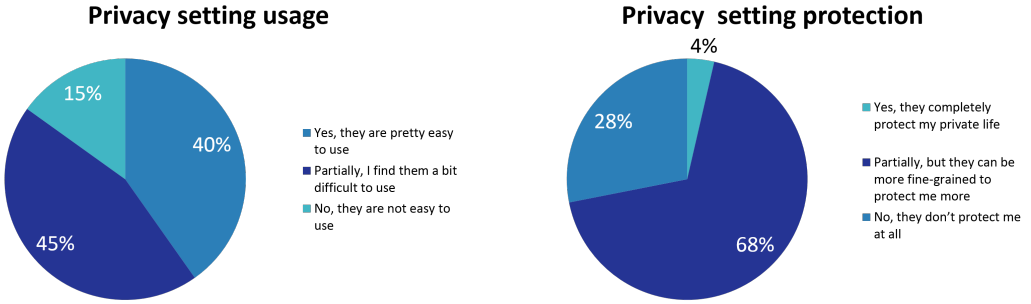


FIGURE 3.5: Privacy settings preferences

3.3.7 Users Preferences for Data Collection

Most of OSNs collect, store, process and analyze user's data and sometimes sell it to third parties for advertising and marketing purposes. New laws and regulations have been enacted to control data collection and enhance privacy protection.

In this study, we asked our participants if they are aware that OSNs are collecting their data and only 14% were knowledgeable of it, while 56% claimed that they know that OSNs are collecting data but they did not know what they are used for, and 30% of the participants did not know that their data is collected when using OSNs services, as shown in Fig. 3.6.

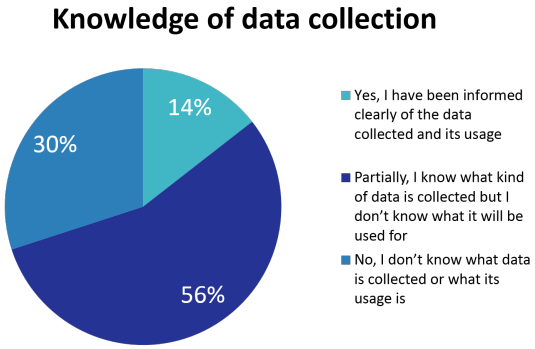


FIGURE 3.6: Knowledge of data collection

Furthermore, 81% of the participants strongly agreed that OSNs should clearly inform users about how their collected data is used and users should decide the usage of their data, and more than 74% agreed that the user should have the ability to choose which information can be shared with OSNs, as shown in table 3.14. They have also ranked location (76%) and personal information (68%) as extremely sensitive and they can have an impact on the privacy of users (refer to table B.14 in appendix B for more information).

TABLE 3.14: Data collection usage

	Inform users		**Usage decision**		**Choose data to collect**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**
Strongly disagree	2	0%	3	1%	4	1%
Disagree somewhat	8	2%	7	1%	13	3%
Neither agree nor disagree	32	7%	28	6%	41	9%
Agree somewhat	47	10%	50	11%	63	13%
Strongly agree	381	81%	382	81%	349	74%

3.3.8 Users Preferences for OSNs' Functionalities

OSNs offer various functionalities and services that attract a great number of users to online social services. The users are instantly informed of news of their interests and their entourage. Each OSN implements different functionalities that make it stand out from other systems. The functionalities are offered to advance and enhance the usability of the systems of sharing digital information (texts, pictures, music, videos, tags, bookmarks, etc.) and for communicating and socializing between users.

We considered the following functionalities in our study: search other users, reshare others' messages, user/content recommender, mention other users, comment on others' messages, and one-to-one messaging with users. The participants agreed that these functionalities are important in OSNs and it will enhance their experience in using OSNs. However, they are not vital to operating in OSNs. Table 3.15 details the answers of the participants.

TABLE 3.15: OSNs Functionalities

	Search others		**Reshare post**		**Recommend**		**Chat**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not important	39	8%	37	8%	54	11%	38	8%
Somewhat important	75	16%	86	18%	95	20%	68	14%
Important	196	42%	179	38%	170	36%	159	34%
Very important	110	23%	102	22%	100	21%	105	22%
Extremely important	50	11%	66	14%	51	11%	100	21%

	Mention		**Comment**	
	Freq.	**%**	**Freq.**	**%**
Not important	55	12%	53	11%
Somewhat important	121	26%	124	26%
Important	158	34%	178	38%
Very important	81	17%	76	16%
Extremely important	55	12%	39	8%

3.4 Summary

This chapter answered two research questions on the information sharing behavior of users and their preferences in OSNs in terms of privacy. The first question investigated the attitude of users towards their information sharing behavior in OSNs, and the factors that influence the sharing behavior. The second question investigated how users perceive OSNs, what are their preferences for an ideal OSN system, and how it should manage with their data and privacy. A sample of 542 participants was analyzed and the results revealed that 13% of the participants do not use any kind of OSNs, mostly for privacy concerns.

In the first question, the focus was put on 7 potential dimensions that might influence information sharing behavior in OSNs: (1) privacy awareness, (2) control of information, (3) data collection limitation, (4) privacy policies understating, (5) privacy settings and functionalities, (6) age, and (7) gender of users. The analysis of the sample revealed that information sharing behavior can be influenced by 4 factors, namely: (1) privacy awareness, (2) control of information, (3) data collection limitation, and (4) granularity of privacy settings and functionalities. In other words, users are more engaged in sharing information in OSNs when they know that they are protected. The analysis also showed that age and gender do not have an influence on the behavior of users in terms of sharing information in OSNs. Women are more concerned and more aware of privacy issues in OSNs than men, but both tend to behave the same way in sharing information. Furthermore, users behave in the same manner when they are sharing their information either with friends or with strangers. In addition to the theoretical study, the findings provide a better understanding of online social providers of how privacy issues can affect the users' acceptance of social networks and their behavior of information sharing.

In the second question, we identified 8 basic components of OSNs: (1) profile management, (2) friendship management, (3) message management, (4) group management, (5) privacy policies, (6) privacy settings, (7) data collection management, and (8) OSNs functionalities. The results showed that users prefer:

- to register in OSNs with an email address and login using pseudonyms and strong passwords.
- only username, email address, and first name are required to create profiles.
- to maintain access to their profile to only their friends.
- to have the ability to accept or reject a new contact, to set the visibility of connections list, and to control who can send friendship requests.
- to maintain the visibility of the connections list in OSNs to only their friends or not be accessible to anyone.
- only their friends who can access to their messages or mention them in messages.
- to have the possibility to share multimedia and to edit and delete published messages.
- to subscribe to a private or semi-private group where posts and member list are viewed only by the members of the group.
- privacy policies should be easy to read and understand

- privacy settings should be fine-grained and easy to configure.
- to be clearly informed about what type of data is collected and for what use.
- to choose what data can be collected and for what purposes.

The results of this chapter will help to derive and analyze the assessment questions discussed in chapter 5. Next chapter, we survey and analyze 24 different OSNs and compared them based on a set of different criteria.

Chapter 4

A Qualitative Comparison of Microblogging OSNs

In this chapter, we survey 24 different OSNs. The systems differ in their design choice, the functionalities they provide, and the security and privacy models they use. We classify the different systems into two classes: (1) deployed systems that are/were operational and they have/had real users, and (2) not deployed systems that are proofs of concepts or proposals in the literature. We evaluate and compare each system based on 7 criteria.

This chapter is structured as follows: Section 4.1 presents and introduces 24 different systems. Section 4.2 presents a set of 7 features and characteristics to compare the surveyed OSNs, namely: (1) the service provided, (2) the architecture, (3) the storage and replication techniques, (4) the encryption mechanisms and key management, (5) the security goals, (6) the privacy goals, and (7) the functionalities. Section 4.3 is dedicated to comparing the systems based on the set of characteristics. Section 4.4 discusses the impact of privacy-preserving techniques on the usability and user-friendliness of systems. Section 4.5 presents a conclusion of the chapter.

4.1 OSNs: THE CURRENT PICTURE

We selected 24 OSNs for our quantitative study. 12 systems are deployed and are used while 12 systems are prototypes for privacy-preserving OSNs exiting in the literature, with a focus on microblogging systems.

4.1.1 Deployed Online Social Systems

In this section, we present a brief description of the 12 MOSNs that are deployed and operational. The systems provide their users with privacy settings to tune the level of privacy desired, and with privacy policies that disclose what is the data gathered and how it is used, managed and disclosed depending on the applicable laws. However, most of the deployed systems retain the right to modify the terms of the privacy policies at any time. In addition, most of the systems generate their revenues by processing, analyzing, aggregating, and selling data. The complete list of the deployed systems is provided in table 4.1. The table presents also the year when the system was built and their last update.

Facebook

It was created in one of the dorms of Harvard University in 2004 [196]. Facebook provides social networking services to its users where they can share their daily life with friends and connections. Currently, Facebook has 2.41 billion monthly active

TABLE 4.1: List of deployed OSNs

OSN System	**Built in**	**Last Update**
Deployed		
Facebook	2004	June 2019
Twitter	2006	June 2019
Jaiku	2006	Not used anymore
Tumblr	2007	June 2019
Plurk	2008	April 2019
Pump.io	2008	October 2018
Diaspora	2010	January 2019
Twitsper	2013	Not used anymore
Twister	2013	October 2018
trsst	2013	Not used anymore
http://gab.ai	2014	October 2018
GNU Social	2014	January 2018

users as of June 30, 2019, which approximately 85% are outside the US and Canada [197].

Facebook uses a centralized architecture with MySQL database infrastructure and Global Transaction ID with MySQL semi-synchronous replication [198, 199], where the availability of the services depends on the single authority of Facebook.

Facebook gives its users the possibility to create accounts, add, accept or decline friendship requests. Users can easily create their profiles providing some personal information like the full name, phone number or email address, etc. Users can post text messages, files, videos, etc. on their wall, and they can reshare or comment on others' posts. They can mention other friends and they can post directly on their friends' walls, provided that they are authorized to do so. Users can also follow their interests by following or creating Facebook pages. Facebook gives its users the possibility to privately chat using instant messaging. Also, it displays recommendation based on the location and interests of users and it gives the possibility to the users to search for a user, a page or a group. Facebook's profile is by default public and anyone on the Internet can access it and see what is shared and the relationship between the users.

The provider assures that all communications between servers and clients are encrypted using HTTPS secure channels. Recently, users have the option to encrypt and authenticate their communications in instant messaging "Facebook Messenger" using AES_CBC and HMAC_SHA256 [200, 201].

Facebook has implemented a real-name policy for user profiles and the policy reads: "You will not provide any false personal information on Facebook" [202]. Facebook provides basic privacy settings for users to choose from, where they can restrict their profile to be private or public and they can choose who can access their profile and see their posts. But, since the architecture of Facebook is centralized and not encrypted, the right to access all information stored in the database stay in the hand of the provider and all deleted contents persist in the backup copies for a period of time, making the act of censorship easier. In fact, in the privacy policies, Facebook states that they retain the right to disable an account if they see it fit [202].

In March 2018, Facebook was involved in a privacy-related scandal. Cambridge Analytica admitted that they harvested up to 87 million Facebook profiles without permission. The data collected was used to build an algorithm to influence voter opinion on behalf of politicians who hired them [21].

Twitter

It is a microblogging service provider, created in 2006 [28]. Twitter allows users to post, retweet, and comment on short 280-character messages called "tweets" [203]. The number of users reaches more than 321 million monthly active users as of the fourth quarter of 2018 [29].

Twitter adopts the centralized architecture and it has built a next-generation distributed database to match their need for availability, scalability and real-time interactions [204]. However, Twitter had experienced many outages concerning availability, as it happened in 2014 after Ellen DeGeneres tweeted an Oscar selfie [205].

Twitter allows users to create profiles by providing personal information like full name and phone number. Most of the information provided in the profile is always public like biography, location, and picture. Users can post photos, videos, and location information. Also, they can mention other users, search for messages related to a certain topic, and they can look for and subscribe to other users' tweets. In this case, the mentioned users will see the message in their timeline although they do not follow the sender. Users can also search for messages related to a certain topic, and they can subscribe to other users' tweets. People may also find other users through third-party services that have been integrated with Twitter. The Twitter's interface displays a list of trending topics on the sidebar along with recommended contents or potential followees.

Twitter uses Transport Layer Security (TLS, formerly SSL) to secure the communications between the clients and the servers, and it provides an optional verified Twitter account where the user can submit a request to authenticate the identity of the person or company that owns the account [206].

Twitter was not built with the privacy protection of users in mind. The profile, tweets, and list of followers are public by default and accessible to all the Internet. But, users can restrict message delivery to just their followers or to just one follower in the case of direct messages. However, Twitter retains the right to access the data stored and analyze its contents to ban abusive and offensive hashtags or users [207].

Twitter suffered from multiple attacks and breaches. In 2017, a vulnerability was exploited in a popular tool called "Twitter Counter". This third party application analyzes Twitter feeds and provides usage statistics (recent Twitter visitors and number of followers). This hack has led to taking control of hundreds of high-profile Twitter accounts like the European Parliament, UNICEF, and Amnesty International [208].

Jaiku

It was developed in 2006 as one of the first competitors of Twitter offering microblogging services. Jaiku was acquired by Google in 2007 [209]. The number of users is not known as Jaiku was shut down in 2012 [210]. Jaiku was based on a centralized architecture where centralized databases were responsible of storing profiles and data of users.

Jaiku allowed users to create profiles, to send and comment on posts, to mention other users and to tag interests. The posts were limited to only 100 characters.

Jaiku released an API that allowed programmers to integrate Jaiku services in their software. It offered also Lifestream, a feedstream service to share online activities [211].

The profiles and posts were by default public and visible to everyone, but the users had the option to make their posts private to only their subscribers.

Tumblr

It is a popular online social networking website [212] with more than 463 million active users by April 2019 [213]. Tumblr is operational since 2007 and owned by "Yahoo!" from 2013 until 2017[214]. Since 2017, Tumblr along with Yahoo is part of Oath Inc. [215].

The platform uses a centralized architecture with Redis, HBase and MySQL [216] and Multi-source Replication from MariaDB [217] to protect the availability of their services.

Users are able to post texts, images, video, quotes, or links to their blogs, to comment or share others' posts, to tag interests, and to mention or search other users. The profiles in Tumblr are by default visible to all Internet. Since 2014, Tumblr released a new update that allows the users to hide their blog from the web and be only viewed by the users of Tumblr.com [218]. Tumblr gives recommendations on possible friends or interests to its users based on their previous activities. The system uses TLS to secure communications between the clients and the servers.

Tumblr's users can restrict the accessibility of their blogs. The users can hide their blogs from public search. Yet, the profile and all the posts shared on the blog are visible to the other Tumblr users even if they are not in the followers' list. Tumblr collects personal information such as name, age, email address, location, and financial information, like credit card number, type, expiration date or other financial information as stated in their privacy policy [218].

In 2013, Tumblr revealed that the site was breached affecting 65 million users' email addresses and passwords [219]. The hacked data was sold on the dark web.

Plurk

It is an OSN that provides microblogging services, launched in 2008 [220]. It allows its users to send short messages (up to 210 text characters in length), links, videos, and photos. It's estimated that Plurk has more than 1 million active users of which 66% are from Taiwan [221]. Plurk uses a centralized architecture where the data (users' profiles, messages, IP address) are stored in MySQL databases.

Plurk allows users to create profiles using personal information such as full name, email address, and birthdate. To add friends, users send friendship requests to establish a mutual relationship, but they can also follow others without their prior permission. The users can send messages to individuals or to groups using instant messaging. Users can reply, reshare posts, or mention other users and tag their interests. Plurk also provides a mechanism to recommend or search for other users or interests. All communications use HTTPS secure channels.

Plurk gives its users the ability to choose to allow everyone to see their profile and timeline or make the profile and posts visible only to friends. They have the possibility to send anonymous posts, but all data are stored at the level of centralized databases making the service susceptible to censorship.

Pump.io

It is an open source censorship-resistant social network that provides microblogging services [222]. It was known previously as Identica.ca [223] but since 2013, Identica.ca has stopped accepting new registration and migrated to pump.io.

Pump.io uses a distributed architecture with a federation of servers. Users can choose where to sign up, and save their data. Users might also build their own server and host the services of the social network.

Users of Pump.io can send messages, comment or share others' messages, tag interests, and search interests and users. By default, a post is only visible to the users' followers. The users can make the post visible to everyone on the Internet by including 'Public' in the 'To:' box. The communication between servers is secured using TLS certificates.

Pump.io has the ability to hide the profiles and data from the general public in case the users opt to create their own servers. Otherwise, the administrators of the servers have read and write rights to access the data stored on the servers.

Diaspora

It is the first federated, user-owned OSN that is deployed and operational since 2010 [224]. Diaspora has more than 1 million active accounts and it grows continually [225]. Diaspora is based on the free Diaspora software [226].

Diaspora has a federated architecture, which allows users to create their own server/pod and host their accounts. The users can choose also to create their profiles on an existing pod. They can choose a pod based on the physical location, the frequency of updating software version, the domain name, or the ratings of the pod. Users can join a pod that is open as they can join a closed pod upon receiving an invitation. To ensure the availability of the data, the Diaspora network distributes data replicas to multiple pods.

User's profiles have a public part (name, interests, and photo), and a private one which is only visible to people which the user authorizes and it contains detailed information (biography, location, gender, and birthday),. In Diaspora, it is possible to follow another user's public posts without the mutual following requests required in some other social networks.

Diaspora offers two options to publish posts: either (1) publicly where any logged-in user can comment on, reshare, and like the public posts or (2) privately where only followers placed in an authorized group can comment on and like the private posts. Private posts are not resharable. Posts in Diaspora can include mentions and interests. Diaspora offers also instant messaging services called conversations where users can send private messages.

Diaspora uses Pretty Good Privacy (PGP) where a unique public/private key pair and an ID called guid are assigned to every user created on a pod. The pod is the one in charge of encrypting and decrypting requests before passed to users.

Diaspora focuses on three aspects to offer to its users: (1) censorship resistance, (2) privacy and control of data, and (3) the freedom to choose what and with whom to share posts. The administrators of pods have read and write access rights to the unencrypted data stored on their pods [227].

Twitsper

Singh et al. introduced Twitsper [228], a wrapper over Twitter that provides privacy controls to the users of Twitter. Twitsper was built on Android in 2013 to protect

Twitter users' browsing habits and routines and at the same time to preserve the commercial interests of Twitter.

To be compatible with Twitter, Twitsper uses the same centralized architecture adopted on Twitter. In other words, users can preserve their privacy while sharing updates on Twitter without migrating to a new application or a new OSN. The private messages in Twitsper are called whispers. Twitsper considers one to one messages technique to send whispers to a group. The users' profiles and whispers are stored on Twitter's servers while the Twitsper's servers store, in MySQL databases, the mapping between the hashed message IDs and the list of users involved in the chat group. The availability of Twitsper relies on both the availability of Twitter services and the Twitsper's server. In case the Twitsper's server is offline, the users can continue using Twitter's services normally without the privacy option. The system puts its trust on Twitter servers not to leak the user's private information.

In Twitsper, the users continue to have the same functionalities that Twitter offers: create profiles (public or private profiles), follow interests, post, comment, share tweets with one or a group of followers, search for content or users, and get recommendations. Besides, it offers the whispers to its users.

The Twitsper system uses TLS certificates to validate the server's authenticity. To hide the identities of the users involved in a whisper from Twistper's servers, the list ID is encrypted with a group key using AES. The recipients of the whisper derive the group key from each message. So, even if the group key is exposed at any moment of the conversation, it does not reveal the old nor the future messages sent to the group. The groups in Twitsper are created and administrated by the users. To reply to a whisper, the user replies only to an intersection between the members of the recipients of the original message and her/his followers, then sends a direct message as a reply to all the users in the intersection. In doing so, the user has restricted the visibility of the reply to only the followers s/he approved of.

Twister

It is an open and free platform, operational since 2013 with 10000 registered users up to date [229]. It offers microblogging services to its users. Twister has a decentralized architecture composed of three overlay networks: (1) a user identity creation and authentication network based on the Bitcoin protocol, (2) a Distributed Hash Table (DHT) overlay network used for resource (i.e. avatar, profile) storage and retrieval, and (3) a collection of disjoint groups of followers network used for notification delivery [230]. The messages of the users are stored in two networks: (1) a short-lived value stored in a DHT network and (2) an archive file similar to BitTorrent network.

Twister uses the blockchain mechanism to create the users' profiles and to guarantee their uniqueness. To propagate user's posts, Twister uses BitTorrent, and anyone who joins a user's torrent can follow the posts. Followees are not notified and do not need to authorize the followers. The users of Twister can send messages to read-only users or to a group of followers. They can send also direct messages (DM), provided that the recipient is a follower of the sender. The followers can also reply to a post, tag a topic, or mention a user in a post, but they can not republish posts of other users. The system provides its users with the option to search for arbitrary words, but not with a recommender.

Twister ensures the anonymity of the senders and prevents identifying the users by forwarding the posts using a number of intermediate nodes before reaching its final destination.

Twister is designed to protect the freedom of speech and the anonymity of user's activities in the platform, also it's censorship-resistant since there is no central authority to administrate the system. Twister uses ECIES (Elliptic Curve Integrated Encryption Scheme) to end-to-end encrypt the data of users and to digitally sign messages ensuring the authenticity and the integrity of users [231].

Trsst

It is a Twitter-like microblogging system [232], deployed as an alpha test in 2013 [233]. It adds encryption, anonymization and censorship resistance to protect the privacy of its users.

Trsst uses a distributed network where a federation of servers agrees to store and propagate the feeds to users. Trsst's users have the possibility to create standalone client nodes and store their profiles and feed or they can contract with an existing server, known as the home server to store the keystore, the feeds, and the attachments. A copy of the stored data is sent to Trsst hub (home.trsst.com/feed) for replication [234].

To create one or more accounts, a user first creates and encrypts a keystore with a password. This latter is used to access and modify the keystore. The user then generates a keypair, and stores it in the keystore. The users of Trsst may optionally attach personal information to their account, such as name, nickname, image, etc.; the users also have the choice to remain anonymous. The users can send, comment and share texts, images, videos, or files with everyone or with only one person in case of the instant messaging mode. Trsst offers the possibility to search for users knowing their IDs (the users' public key). Also, users can follow and mention other users or tag interests in their posts. Trsst can recommend a list of other users to follow.

Trsst uses both public-key and symmetric cryptography to protect the security of contents from censorship. Trsst uses a crypto-currency system such as Bitcoin to generate the keypair. The account's private key is kept in the keystore. To encrypt a message, the user generates a new AES-256 key and uses it to encrypt the message, and then s/he encrypts the generated key using ECDH (Elliptic curve Diffie–Hellman) and appends it to the encrypted message [235]. The result is encrypted with the intended recipient's public key. All client-to-server and server-to-server communications are conducted over HTTPS channels and all public posts are digitally signed.

Even if Trsst promotes the protection of the privacy of users, it is still suffering some aspect that might endanger the security and the privacy of users. In fact, Trsst users' profiles are public to anyone who knows their IDs and also a user can start a conversation with others without following them. Moreover, the list of followers is available to the public, and anyone on the Internet that knows the user's ID can check his/her posts unless the post is private.

Gab.ai

It was launched in August 2016 [236] and has 215,000 active users [237]. Gab offers microblogging services that allow users to post, reply, and republish short messages called gabs. Gab comes in two versions: the free and limited Gab and GabPro. GabPro is a paid and more elaborated version that allows users to create lists, use private group chats, and to go live [238].

Currently, Gab uses centralized architecture to store and replicate data on servers. However, the creators of the system have announced that they will change the architecture in the near future to a decentralized architecture in order to build a true censorship-resistant and community-powered system [237, 239].

Gab has become open to the public recently as it was limited to join by invitation before. The users can create a profile using a username, password, and an email. They can choose to make their profiles public or private. Once the account is created, the users can add new followers and they can send, quote a post, tag an interest, or mention another user. Gab enables its users to share up to 300 characters in one gab. The system's dashboard comes with a search box in order to search for other users and interests, and it recommends potential friends and hot topics. The messages sent by users and the lists of followers and followees are public and visible to any user of Gab. Traffic between clients and servers is encrypted using TLS to secure the traffic between the clients and the servers.

Gab was built with the idea of providing freedom of speech and thought. But, Gab service retains the right to store and administer users' data. In fact, it banned the first Gab user in January 2017 [240].

GNU Social

It is an open source program offering microblogging services [241]. GNU Social was developed for the first time in 2010 and was known under the name of StatusNet project. GNU Social offers similar functionalities like Twitter, but in an open and collaborative environment where the users are in control of their data.

GNU Social uses a distributed microblogging platform and it has 301 online and active servers to supply thousands of users [242]. GNU Social is composed of multiple instances, the current number of running instance is about 50 instances like Quitter.es, gnusocial.de, loadaverage.org. The instances are independent and they communicate with each others using OStatus standard [243].

GNU Social's users can create profiles using a nickname, email address, and password. They can choose to create an account in any instance and they can communicate, follow and be followed by users from other instances. They can also choose to keep their profile visible and searchable to all Internet users as they can limit the access to only the users of GNU Social. They have the right to choose who can follow them and who can read their posts. The users can send texts, files, images, videos, and audio to all GNU Social users, to private groups, or only to one individual as a direct message. The users can share and comment on a post and they follow an interest.

GNU Social focuses on availability and censorship-resistance. The fact that there is no central unit that can bring down the whole network or censor the content of messages reinforces the GNU Social's position in protecting the freedom of users. Also, the system uses secure channels between users and servers and between servers.

However, GNU Social suffers from privacy issues. Actually, the activity of users is public on their timeline and the lists of followers are disclosed to anyone even the unregistered users. GNU Social also lacks controls to protect the integrity and the confidentiality of users and posts from the administrators of the instances, considering that data are stored in clear in the databases. In fact, the administrators can have access to the users' posts, they can read or delete them, and they can even ban a user from using the services of GNU Social.

4.1.2 Non Deployed Online Social Systems

In this section, we present a brief description of 12 OSN systems that have been proposed in the literature. These systems are proposed to address security and privacy issues in OSNs and protect users' data from privacy breaches. The complete list of the not deployed systems is provided in table 4.2. The table presents the year of when the proposed systems were published.

TABLE 4.2: List of not deployed OSNs

OSN Proposal	**Published in**
Not Deployed	
PeerSon	2009
Safebook	2009
FETHR	2009
Megaphone	2010
LifeSocial.Kom	2010
Cuckoo	2010
Vis-à-Vis	2011
Garlanet	2011
HummingBird	2012
DECENT	2012
Cachet	2012
Twitterize	2013

PeerSon

It is a decentralized OSN that provides encryption and access controls coupled with a peer-to-peer (p2p) approach to replace the centralized authority of classical OSNs [244].

In the proposed version of PeerSon, the developers suggested using open DHT for the lookup service to store the data, and to replicate the social links and digital personal spaces (i.e. timeline, posts) in other nodes.

PeerSon proposed to use e-mail addresses as unique identifiers of the users. In order to prevent a malicious DHT-node from collecting e-mail addresses, PeerSon computes a user ID based on the hash of the e-mail address. The users can look for a specific user to follow using the lookup service directly to get all the necessary information. They can post and reply on messages and the can also control who reads and replies on their messages. PeerSon uses public key cryptography to encrypt the messages with the target peer's public key, hence the messages are only accessible to those who have the right keys.

Safebook

It proposes a distributed microblogging system to protect the privacy and the availability of the messages. Cutillo et al [245, 246, 247] proposed a three-tier architecture for Safebook:

1. The first tier, called Matryoshkas, handles communication's privacy, data storage, and availability of data.

2. The second tier is a peer-to-peer (P2P) overlay that provides the application services (e.g., lookup service, identity management service, etc...)

3. The third tier is a Trusted Identification Service (TIS) that provides each user with a unique identifier and public/private keys.

To join Safebook, a user needs an invitation from an already registered user. The new user provides her/his identity set and a proof of owning it and generates a public/private key pair. Then the TIS computes a unique identifier and generates a certificate associating the public key of the user with the identifier. Once the new user is registered in the system, s/he can start the process of creating her/his Matryoshka by sending friendship requests. Each new friend is associated with a trust level with appropriate privileges to who can access the user's profile and read her/his posts. The users in Safebook are notified about a new friend request and they can accept it or discard it. When the request is accepted, the two friends exchange their respective certificates to start communicating. The users can share text messages publicly if the post is tagged public or only with a group of chosen friends if the post is tagged private. The users can also comment or republish messages.

Safebook provides end-to-end confidentiality, authentication, access control, censorship resistance, data integrity, and data availability. Safebook categorizes data into three types: (1) private data (unpublished), (2) published and encrypted data, and (3) published data without encryption. All exchanged messages are encrypted using the receiver's pseudonym public key and signed with the sender's pseudonym private key. The communication tracking in Safebook is not possible since it was built on the concept of Matryoshka. In other words, the malicious node needs to be the first hop for all requests going from and to a node in the Matryoshka to intercept the communications. Also, the mapping between the user's identifier and the pseudonym is only known to the TIS and the direct first shell of friends.

FETHR

Sandler et al. [248] proposed a new infrastructure to integrate microblogging services called FETHR (Featherweight Entangled Timelines over HTTP Requests). FETHR enables users to communicate with each other on top of HTTP with messages of more than 140-byte payload.

FETHR proposes a decentralized architecture where users' data are stored locally on each peer's machine and new messages are gossiped to the followers using a lightweight HTTP-based protocol.

Each user has a canonical URL that serves as a unique ID. This URL contains the user's profile with the personal information and the messages published. The canonical URL is public and searchable by any other user. Followers can subscribe to another user's update simply using HTTP GET and POST messages. FETHR uses a gossip-based update propagation technique where the message's publisher pushes the update to a subset of the followers, who in turn push the message to the rest of the network. The gossip technique plays a role in the distribution of messages and also in the protection of the data against suppression.

The objectives of FETHR do not include privacy preservation controls, it is concerned more about the availability, the authenticity, the integrity, and the completeness of messages. Also, FETHR uses some cryptographic measures such as hash

chaining and digital signature to preserve integrity, but they are not detailed. The decentralized architecture of FETHR ensures that the system is censorship resistant and not reliable on any single service.

Megaphone

It is a proposal of a multicast microblogging system based on a peer-to-peer network [249]. Megaphone organizes the social graph of users in multicast trees where a "poster" node is the root of the tree, and a "follower" is the child node.

The storage of data is performed at the level of the roots and replicated in child nodes. With the decentralized architecture, Megaphone ensures that the system is censorship resistant considering that there is no central authority responsible for administrating the service.

The poster creates the tree, manages the join requests and the list of followers, stores the public keys of child nodes, and sends messages to all nodes in the tree. The poster has the right to accept or discard the new join request. A follower can post a response to a message from the poster, and optionally encrypts and signs it.

Megaphone uses public key cryptography based on RSA. The poster generates session keys to encrypt the messages. The session key is cached by all nodes of the multicast tree, and readable only by the nodes that have registered a public key with the poster. The poster might add a serial number to detect lost messages.

Using the multicast architecture, Megaphone protects confidentiality, integrity, and availability of data. Megaphone protects also the identity of users since the IDs are not based on any piece of information related to the users' real identities, but rather on their public keys. However, the followers inside the circle of the multicast trees can know the source of the posts and who is currently following the poster.

LifeSocial.KOM

It is a decentralized OSN based on peer-to-peer network [250]. It was built to offer the social functionalities of an OSN, with a fault-tolerant and data storage efficiency.

All personal information and shared messages in LifeSocial.KOM are stored in the peers. It provides data availability using the replication mechanism offered by PAST [251]. PAST is an Internet-based, peer-to-peer global storage utility that aims to provide strong persistence, high availability, scalability, and security.

The users of LifeSocial.KOM can create profiles, manage the followers' lists, create, join and manage groups, follow interests, share text and photos, search for people with common interests, browse through pictures of friends and interesting people, and live chat with their friends. The profiles and the posts of the users are only visible to the friends.

LifeSocial.KOM focuses on providing confidentiality, availability, and access controls to its users. It uses public key cryptography for authentication (the public key is used as a unique ID of the users) and a symmetric cryptographic key is used for encryption. LifeSocial.KOM suggests a user-based access control to access the system where users can control who can read and access their data. [252]. Leveraging the decentralized architecture of P2P networks, LifeSocial.KOM protects against censorship since no central authority is responsible for providing the service.

Cuckoo

It was proposed in 2010 by Xu et al [253, 254]. Cukoo is one of the earliest microblogging systems that leverage the decentralized architecture of peer-to-peer networks.

The architecture of Cuckoo is hybrid, meaning it's composed of a small base of servers named server cloud and client peers. The server cloud is used for storing resources like users' profiles and served also as a backup for replication to guarantee the availability. The client peers are served as an overlay of the messages. The server cloud is used for storage of profiles and does not intervene in the message exchange between peers.

The profiles and messages sent by the users are public. Anyone can search for information about any other user. Cuckoo gives its users the possibility to organize their social relationship into friends (the two users reciprocate the social link between them) and neighbors (users who serve as an overlay to disseminate messages based on gossip protocol).

Optionally, Cuckoo uses asymmetric key cryptography to encrypt and to sign the messages. The public key is stored on the server cloud while the private key is kept secret in the client peer's machine. The users can obtain the public keys of the followers either out of band during the following process or from the server cloud.

Cuckoo focuses on providing a microblogging system that is scalable, reliable and censorship-resistant. In fact, Cuckoo protects the users only from censorship since the server cloud is used for storage of profiles and does not intervene in the message exchange between peers. However, Cuckoo does not take the privacy protection of the users into consideration.

Vis-à-Vis

It is a decentralized framework for OSNs based on the privacy-preserving technique of a Virtual Individual Server (VIS) [255, 256]. VIS is a highly available virtual machine running in a paid compute utility, like Amazon EC2, which does not have any claims over the contents stored in the machines. VIS is used to store the users' personal data and posts.

The communication between users is conducted in groups where they can share posts and follow interests, but they can not comment or republish the posts. Each group of users consists of an administrator who creates and manages the group, the members (other users), and the mapping of members in geographic regions. Each member maintains an attribute within the group such as the relationship with the administrator or an interest in a particular topic. Users also have the option to search for a group or a user in a particular region, but the system does not provide any recommendations of available groups or users.

Vis-à-Vis uses public-private key encryption, where users are defined by a self-signed key pair. The public key is used to encrypt the messages and the private key is stored securely in the VIS and it is used for digital signature and decryption of encrypted messages. The public key of a user and the corresponding IP address of the VIS are distributed out of band.

Vis-à-Vis is concerned mainly by the AIC triad (availability, integrity, and confidentiality) of security more than privacy. In fact, VIS administrators can access to all users personal data stored on their machines, but the intermediate computers can only access the ciphered data and some other control data (users' ID and timestamp). Thus, VIS owners need to manage securely their machines, keep them up-to-date, and implement the appropriate access controls policies.

Garlanet

It is a privacy-preserving microblogging system developed at Universitat Oberta de Catalunya (UOC) [257]. It is a collaborative system where the registered users are voluntarily contributing to the computational resources.

Garlanet uses a hybrid architecture composed of a directory service and clients' peers. The directory service is used for lookup services and location data. Users' data are hosted on any resources provided by any users of the system. To ensure the availability of the service and data, Garlanet replicates the data of users on different machines.

Garlanet offers its users the possibility to stay connected with their followers and to express themselves in a censorship-free system. Users can share their activities and interests with their followers and they can also follow other users of the system. In Garlanet, the following process is one-sided and is conducted out of band. Users can access only the public information (name, username, and photo) of another user and they can not access the private information provided in the other users' profiles even if they are following them.

Garlanet is a community-owned OSN where no central authority controls the system. It adds built-in privacy mechanisms to guarantee that only the sender and the intended receivers are able to access the information exchanged. These capabilities can protect the end users from the malicious utilization of personal information and from public exposure of sensitive data, and they guarantee the free exchange of information.

Garlanet protects the confidentiality of sensitive data and guarantees the desired level of anonymity of the users. Each user in Garlanet uses RSA to generate two public keys: (1) one to cipher the storage and (2) the other key is used to decipher the user's messages. The friendship relation between users is not revealed to anyone and the users only have the list of the contacts who they are following. The data are distributed in different repositories so an attacker cannot get information by correlating all the actions that a user performs. Also, the intermediate computers only see the ciphered data and some control data such as a pseudonym ID or a timestamp.

Hummingbird

It is a microblogging OSN that imitates Twitter's functionalities while adding privacy-preserving techniques to protect the personal data of users [258, 259]. Hummingbird uses centralized architecture where the Hummingbird Server (HS) handles all the operations of the user's registration and tweets delivery to followers.

Hummingbird introduces the new concept of "follow-by-topic" where users can decide to follow other users on specific hashtags of interest. It also allows users to conceal their interests by following arbitrary hashtags. A follower issues a request to follow a user on a specific hashtag. The following requests are subject to approval. To preserve privacy, Hummingbird does not allow users to reply to a post or reshare it with other followers. The users' profiles are visible to all other Hummingbird users.

Hummingbird uses several cryptographic protocols like Oblivious PRF (OPRF) technique and Blind- RSA for signature. The users are responsible for generating their own keys and distribute them out of band. The keys are stored in HFE (Hummingbird Firefox extension). The proposed architecture does not handle revocation of the following requests.

Hummingbird is concerned mainly about providing confidentiality and authorization. It adds encryption of tweets to provide confidentiality and access lists for users in order to choose who can access their messages. The posts are hidden from the server and all non-followers and the access to them is restricted only to the authorized followers. However, the Hummingbird server has access to users' accounts, the following requests, and the encrypted messages. It can build a full graph of tweeter-follower relations. In addition, the server can learn whether two followers are subscribed to the same hashtag of a given user and it can learn whenever two posts by the same user carry the same hashtag.

DECENT

It is a proposed project for OSNs that suggests to use a fully decentralized architecture and store user data in a Distributed Hash Table (DHT) overlay [260]. Each write operation in the DHT storage requires prior authorization. This authorization does not reveal the social graph of a user. To protect the objects stored in malicious nodes from vandalism and deletion, DECENT maintains several replicas of an object of a node among its neighbor set, providing high availability to users.

A profile in DECENT contains references to biographic information, the list of contacts, a wall, and photo albums. The users can search for a profile using the wall reference. The users can post messages, links, photos or videos, add a comment, refer to an existing object, and mention another user from their list of contacts. Relationships in DECENT are asymmetric and the users assign levels of trust to their followers. The level of trust assigned to a user might not be reciprocated. For example, user A can add user B to her list of contact just as an acquaintance relationship, while user B can label his relationship with A as friendship.

DECENT provides confidentiality, integrity, availability of the message's content, and privacy of user relationships. It uses AES for symmetric encryption, DSA for signatures, and RSA to encrypt the write policy signature key. DECENT uses also an extended version of EASiER [261]. The keys are exchanged out of band.

When creating an object, the sender creates 3 policies related to the object that state who can read, modify/delete, or comment/annotate the content.

Cachet

It is proposed as a performance improvement of DECENT [262]. Cachet maintains the same functionalities and services of DECENT. Similar to DECENT, Cachet uses also Distributed Hash Table (DHT) overlay network to store and replicate data in the selected nodes ensuring high availability of the objects. The data in Cachet are stored in containers that include updates and photos, wall references, and references of other containers. The containers are protected by encryption.

Cachet uses Attribute-Based Encryption (ABE) scheme [263]. All the keys are exchanged out-of-band. The message is encrypted using a symmetric key which in its turn is encrypted with ABE. Cachet uses the digital signature to ensure the integrity of objects. Also, users maintain secure connections with the followers to receive new updates directly as soon as they are released. In this upgraded version, the authorized readers do not have to decrypt all the wall object, but only the most recent updates.

Twitterize

It is a system designed to preserve the privacy of Twitter's users [264]. Twitterize was built to overcome the shortcoming of Twitter in terms of anonymity and confidentiality. It offers the option to send posts anonymously while maintaining the normal Twitter functionalities. Twitterize maintains the same centralized architecture of Twitter. It uses Android SQLite DB to store tweets, cryptographic keys, subscriptions, etc.

To achieve anonymity, Twitterize establishes one overlay network per each hashtag to connect the sender and the receiver. Each overlay contains forwarders (other Twitter' users who are not interested in the hashtag) to mix the tweet and forward it to its destination. The overlay network is also used to send subscription requests [265]. Using this architecture, forwarders can not link between the sender and the receiver, they can only control their local view of the message's flow and they can not learn the origin or the destination of the tweet.

Twitterize gives the possibility to its users to create profiles and to customize the behavior of service based on their preferences (the synchronization times and the frequency of tweets to pull during synchronization). To publish interests, the creator of a hashtag x encrypts and hashes it to create a pseudonym Px for the hashtag, then the publisher can annotate Px to tweets without revealing the hashtag. Twitterize encrypts tweets to obtain confidentiality using AES-128bit in CBC mode. The keys are exchanged via an out of band channels. Also, the users can generate an optional asymmetric key pair to ensure integrity.

4.2 Criteria of Comparison

Increasingly, more sensitive information is shared in OSNs, generating privacy threats, either related to users or to the system provider. We discussed 6 techniques to mitigate these threats in section 2.3.3: (1) anonymization, (2) decentralization (3) encryption, (4) information security, (5) fine-grained privacy settings and access controls, and (6) user awareness and change of behavior.

To understand how the surveyed systems operate and address the issues of privacy, we identify seven main criteria for classification and comparison, inspired by the privacy mitigation approaches: (1) the service provided, (2) the architecture, (3) the storage and replication techniques, (4) the encryption mechanisms and key management, (5) the security goals, (6) the privacy goals, and (7) the functionalities. In the following section, we discuss the set of characteristics we have identified to evaluate and compare different OSNs.

4.2.1 Type of the Service Provided

To compare different OSNs, the first intuitive criterion is the type of services provided by the system. As explained in section 2.1, Online Social Networks provide multiple operations and services for their users. In addition to social networking, OSNs can offer also microblogging services, multimedia sharing, social review, online chatting, etc.

4.2.2 Architecture

The first criterion for comparison is the architecture design implemented by the OSN provider [266]. As explained in section 2.3.3, a form of decentralization can

be an answer to mitigate against the single authority and content control of a system provider, to support censorship-resistant systems, and to provide openness to uses. In other words, the architecture design of an MOSN system has an effect on the privacy of users and data. Systems adopt 3 different types of architecture:

1. **Centralized architecture** is a traditional approach where all functionalities of the systems are centrally owned and managed by a single authority. It has the advantage of the ease of implementation but at the same time, it suffers from the issues of single points of failure and bottlenecks. The centralization of data under a single administration poses serious threats to users privacy and content ownership [267, 268].

2. **Decentralized architecture (federated or totally decentralized)** relies on the cooperation of users. Users' personal data are stored and maintained distributively. This approach is more privacy-preserving and cost-effective [266, 267, 269]. The drawback is that hosting peers might not be always available or can be malicious.

3. **A hybrid architecture** that combines elements from both of the previous architectures to benefit from the advantages of both approaches.

4.2.3 Storage and Replication Techniques

In line with the previous criterion, MOSNs can be compared based on the type of storage. The answer to where is it convenient to store data is related to the architecture design of the system and to the issues of availability, costs and providing trust to users. The storage of data in MOSNs differs from a system to another. In general, there are 4 methods of storing data: (1) on centralized services maintained by a single authority, (2) on federated servers with multiple authorities, (3) on decentralized services, and (4) on a hybrid of centralized and decentralized services where some forms of data are stored on the nodes and other forms are stored on centralized services.

4.2.4 Encryption Mechanisms and Key Management

Another criterion to compare MOSNs is the encryption mechanisms and the cryptographic key management used in the system. Encryption provides a mechanism to provide confidentiality and protect privacy by giving access control to only authorized users. MOSNs rely on different types of cryptographic algorithms: (1) symmetric algorithms with shared-keys known to all stakeholders, and (2) asymmetric or public-key algorithms with a pair of keys (public and private keys).

4.2.5 Security Goals

Protecting privacy in OSNs turns back to protecting information security as well. To understand the challenges brought by MOSNs to the protection of information security, we review the systems based on the AIC triad (availability, integrity, and confidentiality) [59, 57]. We exclude confidentiality as it is examined in the encryption criterion (see section 4.2.4). We add two more goals to understand how the surveyed systems handle the users' identity creation and authentication.

1. **Availability** ensures access to authorized data and resources at any time and from everywhere.

2. **Integrity** ensures the reliability of the data, stored or in transit, and guarantees that any unauthorized modification is blocked.

3. **User's identity creation** ensures the registration in the system.

4. **User's identity authorization and authentication** ensure adequate access to the system.

4.2.6 Access Control and Privacy Settings Goals

Protecting user's privacy requires denying unauthorized entities from learning any data that can reveal identifying information of the user. The more identifiable personal information in the system with less control over information, the greater the chances of privacy issues. In addition, unauthorized entities should not be able to link users with any private information, meaning that the stored data should not leak any useful information. This implies protecting users' anonymity and the need for unlinkability requirement. This aspect leads directly to the need for access controls and privacy settings.

The access control in MOSNs should be fine-grained and the access to data must be only granted by the owner of the information. This criterion is inspired by the mitigation technique of "Fine-grained privacy settings and access controls" in section 2.3.3. Each private information in the system has to be separately managed, but for the purpose of comparison in this thesis, we identified 7 essential privacy controls that are common and generic to all MOSNs systems. The identified controls are derived from the definition of an OSN. In other words, protecting the data in profiles, relationships, and in the contents [270].

1. **Profile visibility by default** refers to the visibility by default of the profile once it is created.

2. **Change the profile visibility** refers to the possibility to restrict the default visibility of the profile.

3. **Visibility of relationship by default** refers to the visibility by default of the list of relationships.

4. **Visibility of posts by default** refers to the visibility by default of a message when it is posted.

5. **Change the posts' visibility** refers to the possibility to restrict the default visibility of a post.

6. **System provider access** refers to if the service provider can access the users' data.

7. **Storage control** refers to if the users have control over the storage of data.

4.2.7 Functionalities

To understand the trade-off between privacy and usability in MOSNs, a discussion of the functionalities provided in a system is needed. To reach and attract more users, MOSN systems can offer multiple functionalities that are unique to the system. In this thesis and in order to compare different system, we chose a set of functionalities that are common to all systems. Boyd and Ellison's definition [5] of OSNs

distinguishes essential functionalities which needed in a system to be considered as an OSN (refer to section 1).

1. **Profile management**: create and manage profiles.
2. **Relationship handling**: add, accept or remove friends/contacts.
3. **Post and view messages and activities**: share messages with the public, a group or privately.

We add to this list a set of 4 extended features that we considered important as they contribute to the usability of OSNs, but at the same time, each functionality presents a risk of some degree on the privacy of users.

4. **Search function**: find other users, word search, search for comments, etc. The search option can raise privacy concerns by reflecting the preferences of users.
5. **Reply and comment on others' posts**: this can reveal the social graph of the users.
6. **Mentioning other users**: this can reveal the social graphs of users.
7. **Follow interests**: this can reveal the preferences of users

4.3 Comparison and Evaluation

This section provides a comparative classification of the set of OSNs described in section 4.1 with respect to the characteristics detailed above. For the rest of the tables, ✓indicates that the corresponding property is present in the discussed system while ✗implies that the property does not exist. N/A means that no information was found about the corresponding property or it was not addressed in the case of proposed OSNs.

4.3.1 Service Provided, Architecture and Storage

The surveyed OSNs differ in the services provided to their clients, in the architecture, and in the way the data are stored. Table 4.3 summarizes the classification of the systems with respect to the three previous criteria.

While the focus of the surveyed systems is on systems that offer microblogging services, some systems offer other services along with microblogging like the case of Facebook, Vis-à-Vis, DECENT, and Cachet.

Most of the deployed social network sites adopt centralized architecture using central databases to store the users' data. The main reason for choosing such architecture is because centralized systems are easy to create and to maintain and they offer better oversight over the data stored. Meanwhile, the decentralized and the distributed systems are more complex and difficult to maintain due to lower level details that should be taken into consideration like resource sharing and communications. However, the single authority provided by the centralized architecture gives the service provider ownership over the user's data stored in the databases which can be used for monetary gain purposes which presents a threat to the user's privacy.

The decentralized and the federated systems benefit from the fault tolerance nature of the decentralized architecture and give the users more autonomy in terms

TABLE 4.3: Classification of OSNs by the service provided, architecture and storage

System	Service provided	Architecture	Storage
		Deployed	
Facebook	Mixed Services	Centralized	Centralized databases
Twitter	Microblogging	Centralized	Centralized databases
Jaiku	Microblogging	Centralized	Centralized databases
Tumblr	Microblogging	Centralized	Centralized databases
Plurk	Microblogging	Centralized	Centralized databases
Pump.io	Microblogging	Federated	Pods
Diaspora	Microblogging	Federated	Pods
Twitsper	Microblogging	Centralized	Centralized databases
Twister	Microblogging	Decentralized	Locally on user's machine
Trsst	Microblogging	Hybrid	Locally on user's machine
http://gab.ai	Microblogging	Centralized	Centralized databases
GNU Social	Microblogging	Federated	Pods
		Not Deployed	
PeerSon	Mixed services	Decentralized	Locally on user's machine
Safebook	Microblogging	Hybrid	Locally on user's machine
FETHR	Microblogging	Decentralized	Locally on user's machine
Megaphone	Microblogging	Decentralized	Locally on user's machine
LifeSocial.Kom	Mixed services	Decentralized	Locally on user's machine
Cuckoo	Microblogging	Hybrid	Centralized databases
Vis-à-Vis	Mixed services	Federated	Pods
Garlanet	Microblogging	Hybrid	Locally on user's machine
HummingBird	Microblogging	Centralized	Centralized databases
DECENT	Mixed services	Decentralized	Locally on user's machine
Cachet	Mixed services	Decentralized	Locally on user's machine
Twitterize	Microblogging	Centralized	Centralized databases

of controlling and choosing where to store their data. When the users opt to host their data on their devices, the system becomes censorship-resistant since no single authority hosts the data and controls the platform. However, in the case of federated systems, the administrators of the pods should ensure the protection of the privacy of the data hosted and the security of the pods. They have to patch, update, and maintain regularly their pods, as well as they need to install and manage security tools (firewalls, antivirus, IDS/IPS, ...) in order to prevent data leakage and potential security threats.

4.3.2 Encryption Mechanisms and Key Management

All surveyed systems offer cryptography mechanisms to protect the security of the messages and the identity of users. A summary of different aspects of encryption mechanisms in the surveyed OSNs is presented in table 4.4.

Some systems propose to use asymmetric encryption mechanism providing a key pair (public and private keys) that can be used for confidentiality and integrity.

TABLE 4.4: Classification of OSNs by encryption mechanism and key management.

System	Encryption Algorithms	Key Management
	Deployed	
Facebook	TLS cert & AES-256-CBC	Keys are device specific.
Twitter	TLS certificate	N/A
Jaiku	N/A	N/A
Tumblr	TLS certificate	N/A
Plurk	TLS certificate	N/A
Pump.io	TLS certificate	N/A
Diaspora	PGP	Keys gen. by users and stored on pods
Twitsper	TLS cert, AES, & SHA512	Group key gen. from content of each msg
Twister	ECIES	Keys exchanged out of band
Trsst	AES-256 & ECDH	Session keys encrypted with ECDH
http://gab.ai	TLS certificate	N/A
GNU Social	TLS certificate	N/A
	Not Deployed	
PeerSon	Public-key crypto	Not detailed
Safebook	Public-key crypto	Not detailed
FETHR	Not detailed	N/A
Megaphone	RSA	Self-signed keys exchanged when joining
LifeSocial.Kom	Session and public keys	Session keys encrypted with public keys
Cuckoo	(Optional) public keys	Keys exchanged out of band
Vis-à-Vis	Public-key crypto	Self-signed keys exchanged out of band
Garlanet	RSA and AES	Keys exchanged out of band
HummingBird	RSA	Keys exchanged out of band
DECENT	AES, DSA, & RSA	Keys exchanged out of band
Cachet	Attribute-Based Encryp	Keys exchanged out of band
Twitterize	AES 128-CBC	Keys exchanged out of band

Other systems use symmetric cryptography to ensure the confidentiality of posts. Meanwhile, most of the deployed systems use TLS certificates to ensure secure channels for the communications between servers and clients. From table 4.4, we can observe that the majority of the not deployed systems give the users the ability to generate their keys and to manage them. However, the generation and the management of keys in the centralized systems are handled by the providers and the keys are centrally stored. In this case, there is a risk that the system might eavesdrop on the users' messages.

4.3.3 Security Goals

When discussing the protection of privacy, usually protection of information security is discussed as well. So when analyzing the privacy of a system, security should be evaluated as well. OSNs need to have robust security features to protect the users' personal data and prevent data leakage. The security goals of each OSN system are summarized in Table 4.5.

All the surveyed systems are concerned with providing the availability of data

TABLE 4.5: Classification of OSNs by security goals

System	Availability	Integrity	ID Creation	ID Verification
		Deployed		
Facebook	Replica in SRV	✗	User's info	Email/phone and pwd
Twitter	Replica in SRV	✗	User's info	Email and pwd
Jaiku	Replica in SRV	✗	User's info	User ID and pwd
Tumblr	Replica in SRV	✗	User's info	Email and pwd
Plurk	Replica in SRV	✗	User's info	User ID and pwd
Pump.io	N/A	✗	User's info	User ID and pwd
Diaspora	Replica in pod	✗	User's info	User ID and pwd
Twitsper	Servers	✗	User's info	User ID and pwd
Twister	Replica in SRV	Digital sign	User's info	User ID and pwd
Trsst	N/A	Digital sign	Key pair	Public key
http://gab.ai	Replica in SRV	✗	User's info	User ID and pwd
GNU Social	Replica	✗	User's info	UserID/email and pwd
		Not Deployed		
PeerSon	Replica	N/A	Hash of email	User ID
Safebook	Replica	Digital sign	TIS assign ID	User ID
FETHR	Replica	N/A	N/A	The canonical URL
Megaphone	Replicat	Digital sign	UserID & keys	Public Key
LifeSocial.Kom	Replica	Digital sign	Key pair	Public key
Cuckoo	Replica	Digital sign	Server assign ID	N/A
Vis-à-Vis	Replica	Digital sign	Key pair	Public key
Garlanet	Replica	Digital sign	UserID & keys	Credentials of the users
HummingBird	N/A	✗	Server assign ID	✗
DECENT	Replica	Digital sign	Key pair	User ID
Cachet	Replica	Digital sign	Key pair	Public key
Twitterize	N/A	Optional	User's info	User ID and pwd

using replication mechanisms. In the case of the systems with centralized architecture, the data are replicated on central services. In the case of distributed and decentralized architectures, data are replicated on pods or on users' machines. Table 4.5 shows also that not all the deployed systems are concerned with the integrity of data except Twister and Trsst, unlike most of the non deployed OSNs that are concerned about protecting the integrity using a digital signature.

The mechanisms of the user's identity creation and verification differ from a system to another, but we can observe that all the deployed systems have implemented an identity creation and verification techniques as a way to protect the identity of users unlike the proposals OSNs where the authentication is based on verification on public keys or canonical URLs. By doing this, the identity of users is kept anonymous and hidden and adversaries cannot link the profile of a user with her real identity.

4.3.4 Access Control and Privacy Settings Goals

The surveyed OSNs provide different privacy settings to control the visibility of profiles and data to the public, to other users, or to the service providers. For the sake of comparison, we chose 7 privacy settings that are primitive and essential for

protecting privacy in OSNs. Table 4.6 summarizes the privacy goals featured in the different OSNs.

TABLE 4.6: Classification of OSNs by access controls

System	Profile VIS	Control Profile VIS	Relationship VIS	Post VIS	Change Posts VIS	Sys access	Users Storage control
			Deployed				
Facebook	Public	✓	Public	Public	✓	✓	✗
Twitter	Public	✓	Public	Public	✓	✓	✗
Jaiku	Public	✗	Public	Public	✓	✓	✗
Tumblr	Public	✗	Public	Public	✗	✓	✗
Plurk	Public	✓	Public	Public	✓	✓	✗
Pump.io	Public	✓	Private	Followers	✓	Admins	✓
Diaspora	Public	✗	Private	Public	✓	Admins	✓
Twitsper	Public	✓	Public	Public	✓	✓	✗
Twister	Private	✗	Private	Private	✓	Admins	✓
Trsst	Public	✗	Public	Private	✓	✗	✓
http://gab.ai	Public	✓	Public	Public	✗	✓	✗
GNU Social	Public	✓	Public	Public	✓	Admins	✓
			Not Deployed				
PeerSon	Public	✓	Public	Private	✗	✗	✓
Safebook	Private	✓	Private	Public	✓	✗	✓
FETHR	Public	✗	Public	Followers	✗	✗	✓
Megaphone	Public	✗	Private	Public	✓	✗	✓
LifeSocial.Kom	Private	✓	Private	Private	✗	✗	✓
Cuckoo	Public	✗	Public	Public	✓	✓	✗
Vis-à-Vis	Public	✓	Private	Followers	✗	Admins	✗
Garlanet	Private	✗	Private	Followers	✗	✗	✓
HummingBird	Public	✗	Public	Private	✗	✓	✗
DECENT	Public	✗	Private	Public	✓	✗	✓
Cachet	Public	✓	Private	Followers	✗	✗	✓
Twitterize	Public	✓	Public	Public	✓	✓	✗

All the surveyed systems are concerned about protecting the users and their data. The systems provide privacy settings to control the visibility of the profile and contents. However, the privacy issues raised are that the visibility is public by default, in other words, for less aware users who do not change the settings, their information and data are public to be viewed by everyone. If the visibility of profile is public by default in some non deployed systems, like FETHR or Megaphone, is because the identity of users is never directly revealed to the supporting server/peers and protected under a pseudonym (public key or URLs provided by the user), protecting the identity of the users.

Furthermore, the users of the systems that have adopted centralized architecture do not have any control over their information. The data stored are handled centrally which makes the censorship of information easy. Unlike the decentralized, the distributed or the hybrid systems that give their users the possibility to manage the profiles and posts and choose where to host the data.

4.3.5 Functionalities

Like any other online platform, preserving the privacy of users in OSNs comes with a price in terms of the ease of use and the usability level of services provided to the users [271]. To qualify an online platform as an online social network 3 essential features must be realized. With this respect, we included 4 other features that we reckon are fundamental to boost the usability and the friendliness of OSNs but at the same time, they present risks of the privacy of users. This section compares the surveyed systems based on the functionalities highlighted previously. Table 4.7 gives a summary of the comparison of the surveyed OSNs.

TABLE 4.7: Classification of OSNs based on the functionalities

System	Profile Mgt	Relations	Post	Search	Reply	Mention	Follow Interests
Deployed							
Facebook	✓	✓	✓	✓	✓	✓	✓
Twitter	✓	✓	✓	✓	✓	✓	✓
Jaiku	✓	✓	✓	✗	✓	✓	✓
Tumblr	✓	✓	✓	✓	✓	✓	✓
Plurk	✓	✓	✓	✓	✓	✓	✓
Pump.io	✓	✓	✓	✓	✓	✗	✓
Diaspora	✓	✓	✓	✓	✓	✓	✓
Twitsper	✓	✓	✓	✓	✓	✓	✓
Twister	✓	✓	✓	✓	✓	✓	✓
Trsst	✓	✓	✓	✓	✓	✓	✓
http://gab.ai	✓	✓	✓	✓	✓	✓	✓
GNU Social	✓	✓	✓	✓	✓	✗	✓
Not Deployed							
PeerSon	✓	✓	✓	✓	✓	✗	✗
Safebook	✓	✓	✓	✓	✓	✓	✗
FETHR	✓	✓	✓	✓	✗	✗	✗
Megaphone	✓	✓	✓	✓	✓	✗	✓
LifeSocial.Kom	✓	✓	✓	✓	✗	✗	✓
Cuckoo	✓	✓	✓	✓	✗	✗	✗
Vis-à-Vis	✓	✓	✓	✓	✗	✗	✓
Garlanet	✓	✓	✓	✗	✗	✗	✗
HummingBird	✓	✓	✓	✗	✗	✗	✓
DECENT	✓	✓	✓	✓	✓	✓	✗
Cachet	✓	✓	✓	✓	✓	✓	✓
Twitterize	✓	✓	✓	✓	✓	✓	✓

We can observe that all the discussed (deployed and not deployed) systems are indeed classified as online social network platforms. They provide for their users with the mechanisms to create profiles, to handle their relationships, and to share

messages or view their friends'/contacts' posts. When it comes to the usability of the systems, the deployed OSNs attract their users by offering a richer variety of functionalities and ease of use, but this can present risks on the privacy of the users. User's social graphs, interests, and activities can be revealed to other users, which with simple data mining techniques more hidden information can be revealed.

As for the proposed systems, not all functionalities are implemented. Some proposals do not support services such as replying or mentioning other users in the posts like the case of Hummingbird, Safebook, Twitterize or Garlanet. This is due to a design choice in order to protect the privacy of users and prevent data breaches resulting from leakage from social graphs or from messages. The non deployed systems focus more on limiting the access and the visibility of user's data to other users and to the service provider.

4.4 Discussion and Analysis

In the previous section, we have compared different OSNs systems based on 7 criteria. We found that all systems are about meeting the privacy principles discussed in section 2.2.1 and protecting the users and their data to some degree. The surveyed systems can be divided into two groups: the ones that have centralized architecture and the ones that opted for federated and decentralized architectures. Some solutions abolished the system provider completely and opted for user-assisted systems where the users choose where to store the data. However, the system can learn the habit of users from the metadata and usage pattern. Meanwhile, the system providers of centralized systems have the full control of data stored as well as the metadata, making the systems susceptible to censorship and the third-party entities can acquire access to users' profile and retrieve private information without the user's knowledge and consent.

Furthermore, all systems implement some kind of encryption, either TLS certificate, public-key, or symmetric cryptography. In some systems, the encryption serves as an identity creation mechanism, thus the user identity is not revealed to other users nor to the system protecting the anonymity of users, e.g. DECENT. In some other systems, the encryption is used to protect the data in transit or at rest, like the case of Twister and Megaphone. In these cases, the adversaries can not decrypt the protected data, but they can still be able to analyze the flow of communication and deduce the communicated parties and the type of data exchanged (text, photos, videos, etc.).

In addition, the surveyed OSNs provide their users with different privacy settings and controls where the users can limit the access to the data and hide their identity, relationship list, and their data contents. If the OSNs provide efficient fine-grained privacy settings and the users properly tweak them, the success of learning private information about a user will be very weak. The proper access controls that deny accessing relationship list will protect the users from mass data collectors (they use crawling techniques and iterate over friends list to discover the connected friends and contacts). In addition, privacy settings can protect the user from attacks generated from connections that aim to access more information than authorized.

Figure 4.1 is a graphical representation of the comparison of the surveyed systems. The figure compares the privacy protection techniques used in a system versus the functionalities offered by the system. It compares also the privacy risks and violations of each system. The figure gives an insight about the level of privacy protection provided in a system versus the privacy risks and violations that the system

suffers from. These risks can be generated either from the functionalities or from lack of protection mechanisms of privacy.

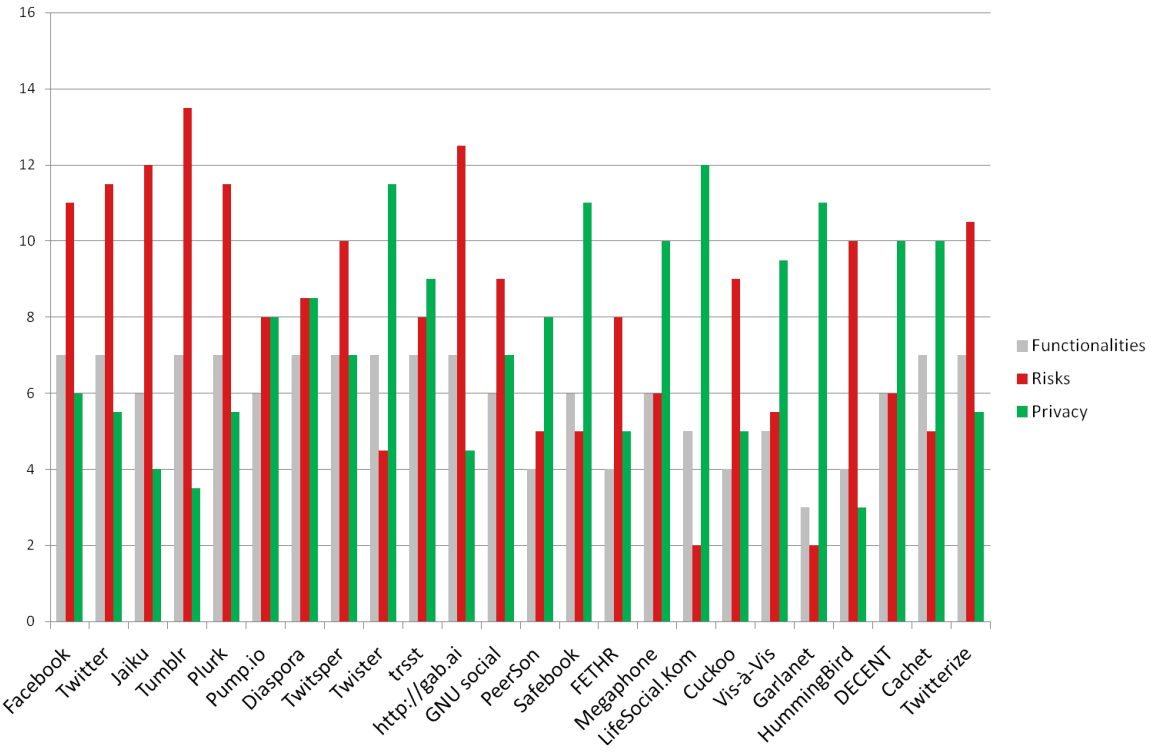


FIGURE 4.1: Comparison of systems based on functionalities, risks, and privacy protection.

4.5 Summary

In this chapter, we have reviewed 24 different OSN systems, with a focus on microblogging systems. The systems are divided into two categories: (i) 12 systems that are/were deployed and operational, and (ii) 12 systems that are proposals found in the literature. We have compared the systems based on a set of 7 criteria: (1) the service provided by the systems, (2) the design architecture, (3) the storage mechanisms, (4) the encryption algorithms, (5) the security goals, (6) the privacy controls implemented in each system, and (7) the functionalities provided. Furthermore, we have presented a comparative evaluation of the surveyed OSN systems based on the security and privacy violations and mitigation techniques implemented. Tables 4.8 and 4.9 summarize the main privacy violations and threats that the surveyed systems suffer from.

Protecting privacy and security in OSNs is a twofold challenge: first, privacy term is ambiguous and its definition differs from a person and from a system to another; second, the concept of OSNs is based on sharing information and various features are continually added to facilitate this for users. The data shared is rich in content and sensitive information about users and their life which risks disclosing their privacy. Vigilance and caution should be taken when implementing privacy protection techniques and approaches. Naive believe of relying on a simple implementation of methods that provide privacy and security in an OSNs cannot protect the privacy in OSNs. Users and system designers should be aware that new security

TABLE 4.8: Main privacy violation in the deployed OSNs

OSN system	**Privacy violations and threats**
	Deployed
Facebook	The data are stored in centralized databases The access control to all data stored is in the hand of the provider The deleted content persist after deletion Easy to ban users and pages
Twitter	The data are stored in centralized databases The access control to all data stored is in the hand of the provider The profiles are public by default and accessible to anyone on the Internet Easy to ban users and hashtags
Jaiku	The profiles and the posts are visible by default and the users can change only the visibility of the posts
Tumblr	The profile and all the posts are visible to the other Tumblr users The data are stored in centralized databases The access control to all data stored is in the hand of the provider
Plurk	The profile and the posts are public by default All data are stored at the level of centralized databases The service is susceptible to censorship
Pump.io	The administrators have read and write rights to data stored on their servers
Diaspora	The profile is public by default The administrators can access the data stored on their servers
Twitsper	The data are stored in Twitter databases and the protection relies on Twitter
Twister	The administrators of the pods can access the data stored The list of followers is public
Trsst	The profiles are public to anyone who knows the users' Ids There is no need to follow a user in order to start a conversation The list of followers is public by default
http://gab.ai	All data are stored at the level of centralized databases
GNU Social	The activity of users is public The list of followers is public to unregistered users The administrators have read and write rights to access the data stored on their servers

TABLE 4.9: Privacy Violation in the non deployed OSNs

OSN System	**Privacy Violations and Threats**
	Not Deployed
PeerSon	The profile is public by default
Safebook	Direct friends can track the sender and the recipient of a message
FETHR	The profile and the posts are public by default Cryptographic measures are not detailed
Megaphone	The followers inside the multicast trees can track the source of the posts and who is currently following the poster
LifeSocial.Kom	The data are isolated from other users and peers access them individually
Cuckoo	The profile and the posts are public by default All data are stored at the level of centralized databases
Vis-à-Vis	The administrators have read and write rights to access the data stored on their VIS intermediate computers can access control data (users' ID and timestamp)
Garlanet	The following is asymmetric and the users can remove a contact from following them
HummingBird	The servers have access all data stored The system can build a full graph of tweeter-follower relations
DECENT	The profile and posts are public by default
Cachet	The profile is public by default
Twitterize	The data are stored in centralized databases The profiles are public by default and accessible to anyone on the Internet

and privacy attacks will materialize every day. Technical approaches are limited if not supported by the awareness of users and legislative measures adopted to OSNs to protect the users.

Hence, there is a need of a formal framework that quantifies privacy and evaluates the performance and the efficiency of the privacy-preserving techniques implemented in OSNs. Chapter 5 provides (i) a guide for the development of privacy metrics and (ii) an algorithmic model to compute privacy scores based on the impact of privacy and security requirements, accessibility, and difficulty of information extraction. Chapter 6 extends the discussion of the present chapter and apply the proposed model to compare between the different surveyed systems.

Chapter 5

IPAM: Information Privacy Assessment Metric for MOSNs

This chapter introduces a novel framework to calculate the privacy score in microblogging Online Social Networks. The framework is comprehensive and generic and it computes privacy scores based on the impact of privacy and security requirements, accessibility, and difficulty of information extraction. The aim of the proposed framework is to provide users as well as system providers with a measure of how much the investigated system is protecting users' privacy. It allows, as well, comparing the privacy protection level between different systems.

For the rest of the chapter, Section 5.1 proposes an approach to develop privacy metrics in MOSNs based on the Plan-Do-Study-Act (PDSA) cycle. Section 5.2 explains the novel algorithmic model to compute privacy score for an MOSN. Section 5.3 presents procedures to compare different systems. Section 5.4 concludes the present chapter.

5.1 Privacy Metrics Development Approach

The proposed framework is designed to guide end users to understand the impact of using OSNs on their privacy. It presents an instrument to measure the privacy level of a MOSN and to compare between different systems. The proposed framework also can be useful for system developers to assess the privacy controls implemented and to have recommendations to enhance the privacy of their systems.

5.1.1 Plan-Do-Study-Act (PDSA) cycle

Plan, Do, Study, Act (PDSA) [272], known as well as Plan, Do, Check, Act, is a well-known iterative approach used to plan and implement a process or a product. The method comprises four steps, as shown in Fig. 5.1:

1. **Plan**: this step is used to clarify the aim and objectives of the defined process or product. This stage includes also defining data and resources to be collected. It results in setting out the outputs and a baseline for improvement.

2. **Do**: it involves collecting data needed for the analysis in the next step.

3. **Study**: this step revolves around converting the collected data into a form that can be used for the next step. It includes analyzing the data and comparing the results with the expected outcomes. It converts the collected data into a form that can be used in the next step.

4. **Act, also called "Adjust"**: results from the previous steps include adjustment or opportunities for improvement should be documented in this step to initiate a new PDSA cycle.

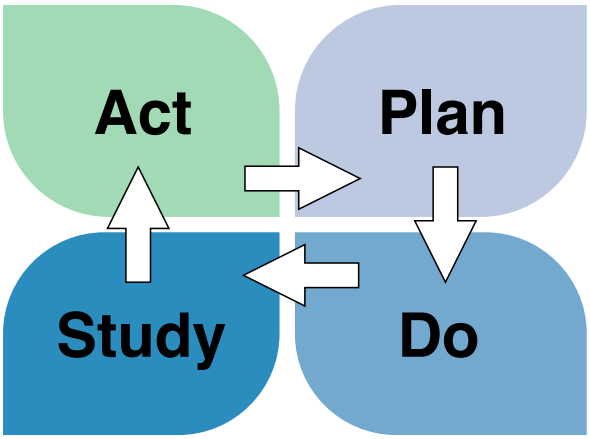


FIGURE 5.1: Plan-Do-Study-Act (PDSA) cycle.

5.1.2 IPAM Methodology

The proposed framework is based on a four-step methodology following the Plan-Do-Study-Act cycle (PDSA). The output is aimed for decision making and for assessing, monitoring, and predicting potential privacy threats in the system under investigation (SUI). It will enable the system providers to gauge how well their system is meeting the privacy objectives, and how well it protects the private data of the users.

- **Step 1 (Plan):** the proposed framework methodology begins by identifying the system under investigation and setting the scope and the depth of the assessment.
- **Step 2 (Do):** this step is concerned with gathering information about the SUI. It starts with a system architecture analysis to identify and understand the system structure, the business processes, the internal and external environment, the key assets and services, the security boundaries, and the implemented controls. Data can be gathered from different sources, including user feedback, risk assessment reports, research surveys, event loggers, etc.
- **Step 3 (Study):** the proposed framework, then, computes an overall privacy score based on the assessment of the impact of information security requirements (availability, integrity, and confidentiality) in addition to the privacy requirements as defined by the National Institute of Standards and Technology (NIST): predictability, manageability and disassociability. The framework answers 4 goals.
  - Goal 1: How the system protects itself from privacy and security point of view.
  - Goal 2: How the privacy and the security of data are handled in the system.
  - Goal 3: How the system protects the users and the data.

– Goal 4: How various assumptions and functionalities provided by the system might affect privacy and security.

This step is detailed in section 5.2

- **Step 4 (Act):** Based on the obtained score from step 3, the framework offers suggestions and recommendations for effectively controlling the privacy of the system.

During the assessment, it can be iterated back to step 2 at any time if the information gathered is not sufficient.

Fig. 5.2 summarizes the flow of the proposed methodology.

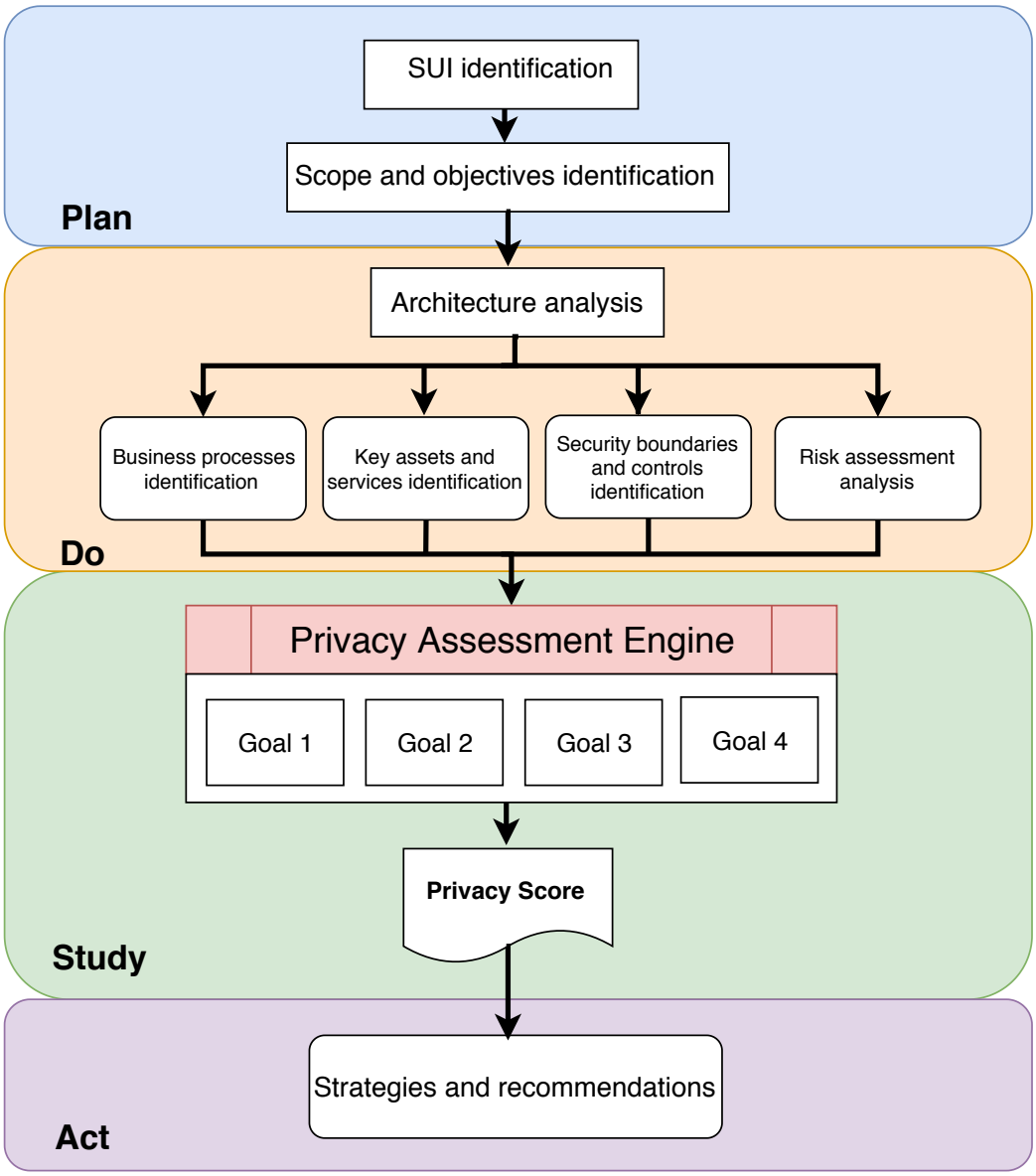


FIGURE 5.2: Framework methodology process.

5.2 Privacy Assessment Engine (PAE)

Once the SUI is identified and analyzed and the data is gathered, the next step is to compute the privacy score. The privacy assessment engine (PAE) represents the core of the framework. It is responsible for analyzing the collected data and computing privacy score for the system. It should be noted that this research does not include methods and technologies to extract and gather information. With these operational characterizations in mind, the privacy assessment engine (PAE) is developed following a Goal-Question-Metric (GQM) paradigm.

5.2.1 Goal-Question-Metric (GQM)

Goal-Question-Metric (GQM) paradigm [273, 274, 275, 276] is a top down derivation and a bottom-up interpretation approach that defines the relationship between the goals and the metrics.

In GQM model, several questions are defined in such a way the metrics answer each question in a quantitative way, which leads to the achievement of the defined goal. GQM defines a measurement model on three levels, as presented in Fig. 5.3:

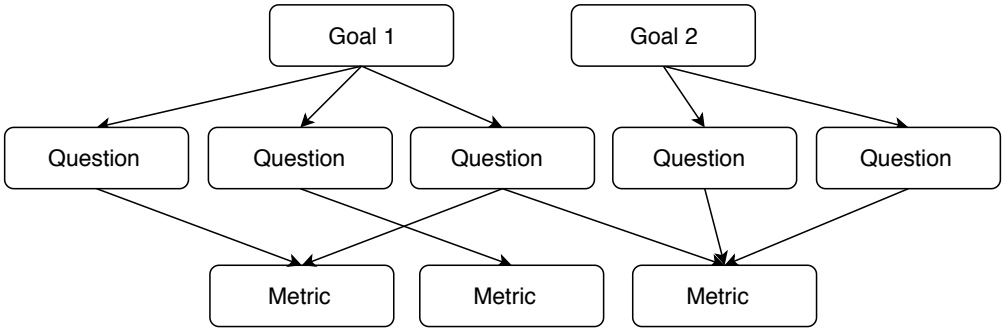


FIGURE 5.3: Goal-Question-Metric paradigm.

1. **Conceptual level (Goal)**: a goal is defined for an object (product, process, resources), from different points of view, relative to a particular environment.
2. **Operational level (Question)**: a set of questions is used to characterize the way the assessment of a specific goal is going to be performed in order to determine its quality from the selected viewpoint.
3. **Quantitative level (Metric)**: a set of measurements associated with every question in order to answer it in a quantitative way. The same metric can be used in order to answer different questions.

5.2.2 Goals of the Framework

Following the GQM model, the goals of the proposed framework are to analyze the SUI for the purpose of assessing and evaluating the level of privacy of:

1. how the system provider protects the users.
2. how the system provider protects the data.
3. how the system provider protects itself.
4. how various assumptions and functions in the system might affect the privacy and the security of the system.

5.2.3 Assessments Questions of the Framework

The assessment questions (AQs) in the framework can be answered as either Yes, No, or Not Addressed (N/A). The questions are designed to cover and counter the known privacy threats and issues in OSNs [277, 278, 71, 104] and they are derived from the set of criteria for classification and comparison discussed in [279]: (1) the type of service provided, (2) the architecture, (3) the storage and replication techniques, (4) the encryption mechanisms and key management, (5) the security goals, (6) the privacy goals, and (7) the functionalities. Furthermore, they are refined from the proposed requirements to protect privacy in social networks [33, 280, 281, 282, 283, 284]. They are also derived in compliance with our definition of privacy as discussed in section 2.2.3.

Since the privacy scores resulted from the framework are used to compare different system, the assessment questions (AQs) are divided into two categories:

1. **Common AQs**: all assessment questions are common and generic to all systems. They are based on the definition of OSNs (refer to introduction 1) and they cover OSNs stakeholders and data as defined in section 2.1.1 and 2.1.2. All the systems should answer the common question and the scores resulted from this set are used to compare different systems.

2. **Specific AQs**: the questions are not common to all systems but specific to only some systems. For example, some systems provide direct messaging while others do not, or some systems provide the functionality of groups while others do not. This set of questions has an influence on privacy (either in a positive or a negative way).

Furthermore, considering that the framework computes an overall privacy score based on the privacy risk present in the system and the privacy protection provided, the assessment questions are formulated in two different manners:

1. **Positive questions (Pos)** are oriented towards privacy protection.

2. **Negative questions (Neg)** have a negative impact on privacy (risk).

Table 5.1 gives an for example of assessment questions. (For a complete list of the AQs, refer to appendix C).

TABLE 5.1: Example of assessment questions

	Assessment Questions (Indicative)
Common	1. Can the unregistered users access the service without creating a profile? 2. Are the friendship requests accepted automatically without consent? 3. Is a new post visible to the public by default on the user's timeline? 4. Can the SUI delete user's data without consent? 5. Are the encrypted communication channel used when transferring data?
Specific	1. Does the SUI add location information by default to the posts? 2. Can users be added to a group without their consent? 3. Can the users mention/tag any other user (non-friends) in the comments? 4. Does the SUI provide users with updates, news and advertisement contents based on their behavior and interests? 5. Does the SUI implement user's feedback about the usability of privacy settings?

5.2.4 Metrics: Theoretical Calculation

Once each assessment question AQ_i in the common and specific set is answered and the result is stored in $AnswerAQ_i$, the framework computes a privacy score from the responses. Table 5.2 presents the notations used in this chapter.

TABLE 5.2: Notation

Notation	Description
TPS	Total Privacy Score
PPS	Privacy Protection Score
PRS	Privacy Risk Score
N	Total number of questions applicable to the SUI
N_{Common}	Number of answered questions in case of common set
$N_{Specific}$	Number of answered questions in case of specific set
N_{PP}	Number of answered privacy protection questions
N_{PR}	Number of answered privacy risk questions
N_{NA}	Number of answered N/A questions
$ScoreAQ$	Privacy score calculated for a question
Imp_{Priv}	Privacy impact score
Imp_{Sec}	Security impact score
AV	Accessibility Value
$Diff$	Data Extraction Difficulty

The privacy score obtained from the proposed framework quantifies the level of the privacy protection provided in a system, under consideration of the existing privacy risk when using the services of the system. In other words, the overall score of an SUI is calculated based on the privacy risk of disclosed information and the privacy protection provided by the system. It is calculated as expressed in (5.1) and it is applicable to both common and specific scores:

$$TPS = \frac{PPS - PRS}{N} \tag{5.1}$$

Where N depends if TPS is a common score or a specific score.

- In case of the common score, all questions are mandatory and should be counted including the questions answered as "N/A". Hence, N is expressed as equation (5.2)

$$N = N_{Common} = N_{PP} + N_{PR} + N_{NA} \tag{5.2}$$

- In case of specific score, N includes only the questions answered as "Yes" or "No", whereas questions answered as "N/A" are ignored, as it is expressed in equation (5.3).

$$N = N_{Specific} = N_{PP} + N_{PR} \tag{5.3}$$

To compute the privacy score PPS and risk score PRS, the privacy assessment engine proceeds as follows:

1. Detect the category of the question (Common / Specific)
2. Detect the type of the question (Pos / Neg)
3. Compute $ScoreAQ$.

    - **Option1. In case of common score**
    $ScoreAQ$ is added to the privacy score PPS if positive questions have positive answers and negative questions have negative or N/A answers. Otherwise, $ScoreAQ$ is added to the risk score PRS if positive questions have negative or N/A answers and negative questions have positive answers. Algorithm 1 explains how privacy protection and privacy risk scores are computed in the case of common questions.

Algorithm 1: Algorithm for computing PPS and PRS in case of common score.

```
i ← 1 while i ≤ numberofquestions do
    if (AQ_i is Pos && AnswerAQ_i = Yes) || (AQ_i is Neg && AnswerAQ_i = No)
      || (AQ_i is Neg && AnswerAQ_i = N/A) then
        PPS = PPS + ScoreAQ_i;
    else if AQ_i is Neg && AnswerAQ_i = Yes) || (AQ_i is Pos && AnswerAQ_i =
      No) || (AQ_i is Pos && AnswerAQ_i = N/A) then
        PRS = PRS + ScoreAQ_i;
end
```

    - **Option2. In case of specific score**
    $ScoreAQ$ is added to the privacy score PPS if positive questions have positive answers and negative questions have negative answers. Otherwise, $ScoreAQ$ is added to the risk score PRS both positive questions have negative answers and negative questions have positive answers. The questions answered as N/A are ignored. Algorithm 2 explains how privacy protection and privacy risk scores are computed in the case of specific questions.

Algorithm 2: Algorithm for computing PPS and PRS in case of specific score.

```
1 i ← 1 while i ≤ numberofquestions do
2     if (AQ_i is Pos && AnswerAQ_i = Yes) || (AQ_i is Neg && AnswerAQ_i = No)
        then
3         PPS = PPS + ScoreAQ_i;
4     else if AQ_i is Neg && AnswerAQ_i = Yes) || (AQ_i is Pos && AnswerAQ_i =
        No) then
5         PRS = PRS + ScoreAQ_i;
6     else if AnswerAQ_i = N/A) then
7         ScoreAQ_i = 0 (Question is ignored)
8 end
```

The process of calculating PPS and PRS is summarized in Fig. 5.4: :

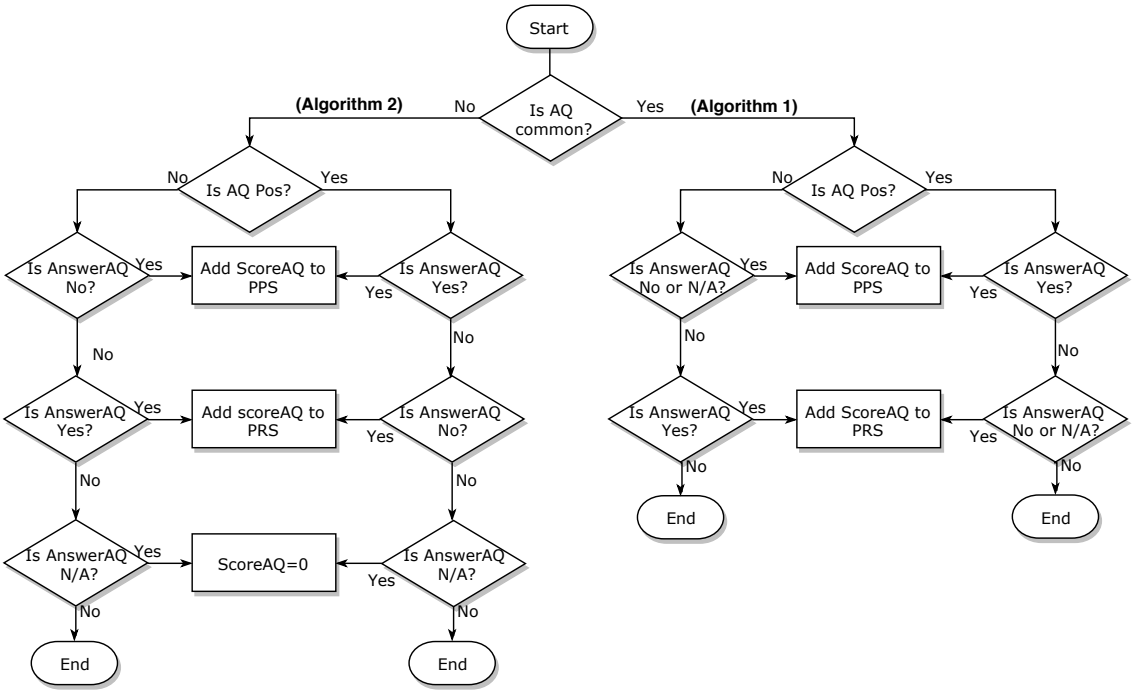


FIGURE 5.4: Privacy assessment engine workflow.

Calculation of ScoreAQ

To compute PPS and PRS, PAE computes a score $ScoreAQ$ that differs for each AQ. This variable measures the impact of the question in terms of privacy, security and visibility and it is calculated as a function of three factors: (i) privacy impact, (ii) security impact, and (iii) visibility as shown in equation (5.4).

$$ScoreAQ = f(Imp_{Priv}, Imp_{Sec}, Visibility) \tag{5.4}$$

The formula to calculate $ScoreAQ$ is based on the privacy score proposed in previous studies [143] and [144] (sensitivity of items multiplied by their visibility). However, in this proposed framework, instead of the sensitivity, we calculate the privacy and security impact of the items. This change was because the impact is

a wider concept than sensitivity, while this later is a property or component of the impact [285].

To calculate the values of the factors to obtain $ScoreAQ$, different sources can be used [286, 287, 288, 289, 290].

1. Calculation of privacy impact

   Privacy Impact score Imp_{Priv} reflects the impact of the assessment question on the privacy. It is calculated as shown in equation (5.5):

   $$Imp_{Priv} = Imp_{Pred} + Imp_{Manage} + Imp_{Diss}. \tag{5.5}$$

   Where:

   - Imp_{Pred}: measures the impact of the question on predictability.
   - Imp_{Manage}: measures the impact of the question on manageability.
   - Imp_{Diss}: measures the impact of the question on disassociability.

   The possible values of Imp_{Pred}, Imp_{Pred}, and Imp_{Diss} are between 0 and 5 as shown in table 5.3. Thus, the value of privacy impact is between 0 and 15.

   TABLE 5.3: Impact value for privacy

Values	Numerical Value
Very High	5
High	4
Moderate	3
Low	2
Insignificant	1
None	0

2. Calculation of security impact

   Security Impact score Imp_{Sec} reflects the impact of the assessment question on the security. It is calculated as shown in equation (5.6):

   $$Imp_{Sec} = Imp_{Avail} + Imp_{Conf} + Imp_{Integ}. \tag{5.6}$$

   Where:

   - Imp_{Avail}: measures the impact of the question on availability.
   - Imp_{Conf}: measures the impact of the question on confidentiality.
   - Imp_{Integ}: measures the impact of the question on integrity.

   The possible values of Imp_{Avail}, Imp_{Conf}, and Imp_{Integ} are between 0 and 5 as shown in table 5.4. Given these ranges of values, the final security impact has a score between 0 and 15.

TABLE 5.4: Impact value for security

Values	Numerical Value
Very High	5
High	4
Moderate	3
Low	2
Insignificant	1
None	0

3. Calculation of visibility

   The visibility score determines how accessible the data discussed in the question. For calculating the visibility, we consider two factors: accessibility and data extraction difficulty. For visibility score, we are using the formulas derived by Aghasian et al [291] The visibility score is calculated as shown in equation (5.7).

$$Visibility = AV * Diff. \tag{5.7}$$

   - **Accessibility** (AV) measures the permissions given to share information with others. In other words, it indicates how many people can access the shared information. The accessibility value depends on whether the score calculated is PPS or PRS. Table 5.5 shows the possible accessibility values.

TABLE 5.5: Accessibility value

Values	AV in case of PPS	AV in case of PRS
Publicly available	1	5
Accessible by friends of friends	2	4
Accessible by system provider	3	3
Accessible by friends	4	2
Not accessible except data owner	5	1
None	0	0

   - **Data extraction difficulty** ($Diff$) measures the difficulty of extracting private information from the formats of data discussed in the assessment question. For calculation of difficulty, 4 levels have been defined from 0 to 3. The extraction difficulty value depends also on whether the score calculated is PPS or PRS. Table 5.6 shows the possible values for extraction difficulty. Naturally, the more accessible an item is, the less difficult is to extract data.

TABLE 5.6: Data extraction difficulty values

Values	$Diff$ in case of PPS	$Diff$ in case of PRS
Low difficulty	1	3
Medium difficulty	2	2
High difficulty	3	1
None	0	0

The value of visibility is between 0 and 15.

4. Calculations of assessment question score $ScoreAQ$

   As expressed in equation (5.4), $ScoreAQ$ depends on three factors (i) privacy impact Imp_{Priv}, (ii) security impact Imp_{Sec}, and (iii) visibility $Visibility$. It is not necessary that all factors are applied in calculating $ScoreAQ$. The assessment questions can have an impact only on one factor (for example only privacy is applicable), or on two factors (for example: privacy and visibility are applicable), or on all three factors (privacy, security, and visibility). Thus, there are 3 cases to calculate $ScoreAQ$.

   (a) Case A: only one factor is applicable (not null)

   $$ScoreAQ = \frac{20}{3} * Factor. \tag{5.8}$$

   (b) Case B: 2 factors are applicable (not null)

   $$ScoreAQ = \frac{4}{9} * Factor1 * Factor2. \tag{5.9}$$

   (c) Case C: all factors are applicable (not null)

   $$ScoreAQ = \frac{4}{135} * \prod_{i=1}^{3} Factor_i. \tag{5.10}$$

   The possible values of $ScoreAQ$ are between 0 and 100. The purpose of the weight added to the equations is to harmonize the score between all the cases since the maximum value possible for each factor is 15.

5.3 SUIs Comparison and Assessment

To understand the overall privacy score obtained in the system under investigation, we compare it against two systems of reference (an ideal system and a flawed system). The systems of reference are hypothetical microblogging systems where the ideal system is 100% efficient in protecting the privacy of users and data, while the flawed system is 100% deficient in protecting privacy. In other words, the total score of the ideal system is based only of PPS ($PRS = 0$), as shown in equation (5.11), and the total score of the flawed system is based only of PRS ($PPS = 0$), as shown in equation (5.12). The total privacy score obtained of every investigated system is between TPS_{Flawed} and TPS_{Ideal} (see (5.13)).

$$TPS_{Ideal} = \frac{PPS}{N}. \tag{5.11}$$

$$TPS_{Flawed} = \frac{-PRS}{N}. \tag{5.12}$$

$$TPS_{Flawed} \leq TPS_{SUI} \leq TPS_{Ideal}. \tag{5.13}$$

To understand further the obtained overall privacy score and to facilitate the comparison between different systems, we convert the values TPS into a percentage (%) ranging between the flawed system (TPS_{Flawed} would represent 0%) and the ideal system (which would represent 100%).

Another type of score evaluation is to compute the accuracy of the SUI. To do so, we compare the SUI against the ideal system based on the answers of the assessment questions for each system (ideal and SUI). We calculate the number of true results where the answers of SUI match the answers from the ideal system (true positives (TP) and true negatives (TN)), as shown in the example in table 5.7.

TABLE 5.7: Example to calculate the accuracy

	Answers in Ideal	Answers in SUI	Outcome
AQ1	Yes	Yes	1
AQ2	Yes	No	0
AQ3	No	Yes	0
AQ4	No	No	1

The accuracy of SUI then is computed as the number of questions that match the answers from the ideal system among the total number of assessment questions, as shown in equation (5.14). Naturally, the accuracy of the ideal system is 100% and the accuracy of the flawed system is 0% (see equation (5.15) and equation (5.16)), while the accuracy of the SUI is between 0% and 100% as shown in equation (5.17).

$$Accuracy = \frac{NumberOfCorrectlyAnsweredQuestions}{N}. \tag{5.14}$$

$$Accuracy_{Ideal} = 100\% \tag{5.15}$$

$$Accuracy_{Flawed} = 0\% \tag{5.16}$$

$$Accuracy_{Flawed} \leq Accuracy_{SUI} \leq Accuracy_{Ideal} \tag{5.17}$$

TPS_{SUI} gives a general overview of the score of privacy level provided in the system under investigation. It can be used by users to compare between different systems and choose the most adequate system based on their necessity. While the accuracy measures to what extent the system under investigation conforms to a standard and how close it is to an ideal system that protects the privacy of users. The result obtained from computing the accuracy can help the developers to compare their system with an ideal one and to evaluate and fix the privacy flaws in the systems.

5.4 Summary

In this chapter, we have presented a comprehensive and generic framework to compute privacy scores in microblogging Online Social Networks. We presented a systematic methodology to develop privacy metrics in MOSNs based on the Plan-Do-Study-Act (PDSA) cycle. Then, we proposed an algorithmic model to compute privacy scores in MOSNs.

The model is based is on the Goal-Question-Metric (GQM) paradigm. We have defined 4 goals to analyze and assess the privacy in terms of how the SUI protects the users, the data, itself, and the functionalities provided that might affect privacy. Then, we derived assessment questions, they are classified into common questions that are generic to all systems and used to compare between different systems and specific questions that are specific to the system under the investigation. The metric developed to compute privacy scores is based on the impact of privacy and security requirements, accessibility, and extraction difficulty of information in MOSNs. Furthermore, the chapter presented two methods to evaluate the obtained scores: the first method is to compare the score against two systems of reference (an ideal system and a flawed system), and the second method is to evaluate the accuracy of the SUI and calculate the number of the answers of SUI that match the answers from the ideal system.

In summary, the results of the proposed framework can be used to obtain evidence of the effectiveness and the efficiency of the privacy mechanisms implemented in the system under investigations. Furthermore, the framework aims to quantify, measure, and evaluate the privacy of the system under investigation and compare between different MOSNs. For the next chapter, we demonstrate the feasibility of our framework using different real social networks and comparing the obtained privacy scores.

Chapter 6

A Quantitative Comparison of Microblogging OSNs

The previous chapter presented the IPAM framework, an information privacy assessment metric to calculate privacy scores in microblogging Online Social Networks. In order to study the applicability of IPAM in the case of real-world online social networks, this chapter describes a feasibility study using the proposed algorithmic model to compare between the systems discussed in chapter 4.

Section 6.1 will follow the framework methodology to obtain privacy scores for each system. Then, Section 6.2 will discuss and compare between the surveyed systems based on the scores obtained from the metric. Section 6.3 will discuss and compare between our proposed framework and related work. While Section 6.4 will conclude the present chapter.

6.1 Information Privacy Scores and Results

To prove the applicability and feasibility of the proposed framework, first we apply the methodology Plan-Do-Study-Act outlined in 5.1 on the online social networks surveyed in chapter 4.

6.1.1 Step 1: Scope and Objectives Definition

The proposed framework is used to assess and evaluate the level of privacy of different microblogging OSNs. The purpose is to assess the privacy issues in each system and to monitor the status of the levels of privacy provided. The proposed framework will facilitate the improvement and enhancement of the privacy level by applying corrective actions, based on the observed results.

6.1.2 Step 2: SUI Analysis and Data Gathering

The second step starts with analyzing the architecture of systems and the functionalities provided. As seen in chapter 4, we have studied 24 different OSNs divided into categories: (1) 12 deployed systems that are in service or were operational and they have real users, and (2) 12 not deployed systems that are proofs of concepts or proposals found in the literature (see tables 4.1 and 4.2).

In this comparison, we consider only 9 deployed systems and 11 non deployed systems. Table 6.1 displays the list of the OSNs considered for this comparison, along with a reminder of the year when the system was built and their last update for deployed systems and the year when the proposals of the non deployed systems were published. The reason we did not consider Jaiku, Twitsper, and trsst is because

they are no longer used, and Vis-à-Vis from the non deployed set is because it does not offer microblogging services, while the focus of the present metric is online social systems that offer among other services microblogging services.

TABLE 6.1: List of OSNs considered in the comparison

OSN System	**Built in**	**Last Update**	**OSN Proposal**	**Published in**
Deployed			Not Deployed	
Facebook	2004	June 2019	PeerSon	2009
Twitter	2006	June 2019	Safebook	2009
Tumblr	2007	June 2019	FETHR	2009
Plurk	2008	April 2019	Megaphone	2010
Pump.io	2008	October 2018	LifeSocial.Kom	2010
Diaspora	2010	January 2019	Cuckoo	2010
Twister	2013	October 2018	Garlanet	2011
http://gab.ai	2014	October 2018	HummingBird	2012
GNU Social	2014	January 2018	DECENT	2012
			Cachet	2012
			Twitterize	2013

The data gathered about the systems is summarized in chapter 4.

6.1.3 Step 3: Privacy Score Computation

As explained in section 5.2, in this study, we derived the assessment questions for common and specific scores. In total, we have 48 common assessment questions and 68 system-specific assessment questions (refer to appendix C).

The questions are divided in the common set into 6 parts: (1) profile, (2) relationship, (3) posts, (4) data storage, (5) data collection, (6) data encryption. The common questions should all be answered with Yes, No, or N/A.

The questions in the specific are divided into 11 parts: (1) profile, (2) posts, (3) groups, (4) data collection, (5) data encryption, (6) functionalities, (7) architecture and application, (8) settings, (9) privacy policies, (8) feedback, and (9) API and third-party relationships. That questions can be answered with Yes or No while the questions answered as N/A are ignored ($ScoreAQ = 0$).

To compute the privacy score for each system, we applied the formulas (5.8), (5.9) or (5.10) to compute the assessment questions scores $ScoreAQ$ in each system. As discussed in chapter5, $ScoreAQ$ is based on the impact of the question in terms of privacy, security, and visibility. The complete lists of the AQ scores are presented in appendix D.

Common Privacy Scores

Following algorithm 1, we calculated the privacy risk score PRS based on how much information is disclosed and the privacy protection score PPS based on how the privacy of users is protected in each investigated system. The results of PRS and PPS are presented in 6.2 for the score of the reference systems, 6.3 for the deployed systems, and 6.4 for the non deployed systems.

TABLE 6.2: Common PPS and PRS for the reference systems

	Flawed system	**Ideal system**
N_{PP}	0	48
PPS_{Common}	0	1475
N_{PR}	48	0
PRS_{Common}	-1314	0

TABLE 6.3: Common PPS and PRS for the deployed systems

	Facebook	**Twitter**	**Tumblr**	**Plurk**	**Pump.io**	**Diaspora**	**Twister**	**Gab**	**GNU**
N_{PP}	19	23	27	28	30	40	40	19	16
PPS_{Common}	497	524	630	635	756	978	1152	600	799
N_{PR}	29	25	21	20	18	8	8	29	32
PRS_{Common}	-619	-716	-632	-539	-533	-279	-273	-597	-569

TABLE 6.4: Common PPS and PRS for the non deployed systems

	PeerSon	**Safebook**	**FETHR**	**Megaphone**	**LifeSocial**	**Cuckoo**
N_{PP}	36	39	36	38	35	18
PPS_{Common}	1041	1110	1029	1096	1034	757
N_{PR}	12	9	12	10	13	30
PRS_{Common}	-387	-228	-404	-310	-384	-523
	Garlanet	**HummingBird**	**DECENT**	**Cachet**	**Twitterize**	
N_{PP}	37	31	36	36	26	
PPS_{Common}	1038	820	1057	1057	633	
N_{PR}	11	17	12	12	22	
PRS_{Common}	-259	-476	-366	-331	-571	

Once the privacy risk score PRS and the privacy protection score PPS are computed for each investigated system, using equation (5.1), we calculated the common overall privacy score TPS for the reference systems, the deployed systems and the non deployed systems, as shown in tables 6.5, 6.6, and 6.7.

TABLE 6.5: Common TPS for the reference systems

	Flawed	**Ideal**
N_{Common}	48	48
TPS_{Common}	-27,38	30,73
Percentage (%)	0%	100%

TABLE 6.6: Common TPS for the deployed systems

	Facebook	**Twitter**	**Tumblr**	**Plurk**	**Pump.io**	**Diaspora**	**Twister**	**Gab**	**GNU**
N_{Common}	48	48	48	48	48	48	48	48	48
TPS_{Common}	-2,54	-4,00	-0,04	2,00	4,65	14,56	18,31	0,06	4,79
%	43%	40%	47%	51%	55%	72%	79%	47%	55%

TABLE 6.7: Common TPS for the non deployed systems

	PeerSon	**Safebook**	**FETHR**	**Megaphone**	**LifeSocial**	**Cuckoo**
N_{Common}	48	48	48	48	48	48
TPS_{Common}	13,63	18,38	13,02	16,38	13,54	4,88
%	71%	79%	70%	75%	70%	56%
	Garlanet	**HummingBird**	**DECENT**	**Cachet**	**Twitterize**	
N_{Common}	48	48	48	48	48	
TPS_{Common}	16,23	7,17	14,40	15,13	1,29	
%	75%	59%	72%	73%	49%	

Specific Privacy Scores

Similar to the common privacy score calculated in the previous section, we calculate the specific privacy scores for the systems under investigation. Using algorithm 2, we calculated the privacy risk score PRS and the privacy protection score PPS for each investigated system. The results of PRS and PPS are presented in 6.8 for the score of the reference systems, 6.9 for the deployed systems, and 6.10 for the non deployed systems.

TABLE 6.8: Specific PPS and PRS for the reference systems

	Flawed system	**Ideal system**
N_{PP}	0	58
$PPS_{Specific}$	0	1838
N_{PR}	62	0
$PRS_{Specific}$	-1766	0

TABLE 6.9: Specific PPS and PRS for the deployed systems

	Facebook	**Twitter**	**Tumblr**	**Plurk**	**Pump.io**	**Diaspora**	**Twister**	**Gab**	**GNU**
N_{PP}	32	34	31	22	20	33	24	27	26
$PPS_{Specific}$	856	983	928	619	600	889	845	838	852
N_{PR}	31	30	23	29	19	14	19	34	30
$PRS_{Specific}$	-882	-827	-532	-713	-462	-317	-491	-959	-815

TABLE 6.10: Specific PPS and PRS for the non deployed systems

	PeerSon	**Safebook**	**FETHR**	**Megaphone**	**LifeSocial**	**Cuckoo**
N_{PP}	7	8	4	20	8	8
$PPS_{Specific}$	161	228	95	633	323	197
N_{PR}	4	3	2	0	3	6
$PRS_{Specific}$	-73	-56	-46	0	-80	-121
	Garlanet	**HummingBird**	**DECENT**	**Cachet**	**Twitterize**	
N_{PP}	19	11	17	17	28	
$PPS_{Specific}$	711	407	589	589	900	
N_{PR}	2	2	1	1	27	
$PRS_{Specific}$	-49	-84	-22	-22	-715	

Once the privacy risk score PRS and the privacy protection score PPS are computed for each investigated system, using equation (5.1), we calculated the common

overall privacy score TPS for the reference systems, the deployed systems and the non deployed systems, as shown in tables 6.11, 6.12, and 6.13.

TABLE 6.11: Specific TPS for the reference systems

	Flawed	**Ideal**
$TPS_{Specific}$	62	58
$TPS_{Specific}$	-28.48	31.69
Percentage (%)	0%	100%

TABLE 6.12: Specific TPS for the deployed systems

	Facebook	**Twitter**	**Tumblr**	**Plurk**	**Pump.io**	**Diaspora**	**Twister**	**Gab**	**GNU**
$N_{Specific}$	63	64	54	51	39	47	43	61	56
$TPS_{Specific}$	-0.41	2.44	7.33	-1.84	3.54	12.17	8.23	-1.98	0.66
%	47%	51%	60%	44%	53%	68%	61%	44%	48%

TABLE 6.13: Specific TPS for the non deployed systems

	PeerSon	**Safebook**	**FETHR**	**Megaphone**	**LifeSocial**	**Cuckoo**
$N_{Specific}$	11	11	6	20	11	14
$TPS_{Specific}$	8.00	15.64	8.17	31.65	22.09	5.43
%	61%	73%	61%	100%	84%	56%

	Garlanet	**HummingBird**	**DECENT**	**Cachet**	**Twitterize**
$N_{Specific}$	21	13	18	18	55
$TPS_{Specific}$	31.52	24.85	31.50	31.50	3.36
%	100%	89%	100%	100%	53%

Accuracy Scores

In addition, we computed the accuracy of investigated systems with the ideal system by applying equation (5.14). Tables 6.14, 6.15, and 6.16

TABLE 6.14: Accuracy for the reference systems

	Flawed	**Ideal**
N	48	48
N º correctly answered	0	48
Accuracy	0%	100%

TABLE 6.15: Accuracy for the deployed systems

	Facebook	**Twitter**	**Tumblr**	**Plurk**	**Pump.io**	**Diaspora**	**Twister**	**Gab**	**GNU**
N	48	48	48	48	48	48	48	48	48
Correct Ans	19	23	27	28	30	40	40	29	32
Accuracy	40%	48%	56%	58%	63%	83%	83%	60%	67%

TABLE 6.16: Accuracy for the non deployed systems

	PeerSon	**Safebook**	**FETHR**	**Megaphone**	**LifeSocial**	**Cuckoo**
N	48	48	48	48	48	48
Correct Ans	36	39	36	38	35	30
Accuracy	75%	81%	75%	79%	73%	63%

	Garlanet	**HummingBird**	**DECENT**	**Cachet**	**Twitterize**
N	48	48	48	48	48
Correct Ans	37	31	36	36	26
Accuracy	77%	65%	75%	75%	54%

6.1.4 Step 4: Comparison and Analysis

Once the privacy scores are computed using the proposed algorithmic model, the framework offers recommendations and suggestions to enhance the obtained score and minimize the privacy risk score. The privacy assessment of the SUIs identifies the risk items that should be addressed by the system provider. It gives also instructions to users about the privacy settings and parameters that should be changed from the default status before starting using the services of the system investigated. Table 6.17 shows an example of recommendations provided by the framework in the case of Twitter.

TABLE 6.17: Example of recommendations for Twitter

Assessment Questions (indicative)	**Answer**	**Recommendations**
Can the unregistered users access the service w/o creating a profile? (Neg)	Yes	Only the authorized users should be able to access the profile
Can the users change the default visibility of the profile? (Pos)	Yes	No Recommendation
Can the users change the visibility of their relationship list? (Pos)	No	Implement settings to restrict the visibility of the relationship list
Is a new post visible to the public by default on the user's timeline? (Neg)	Yes	Post should be private by default
Does the SUI ask for users' consent to collect data? (Pos)	Yes	No Recommendation
Can the users receive direct messages from anyone by default? (Neg)	Yes	DM should be received from only authorized users.
Does the SUI provide privacy policies? (Pos)	Yes	No Recommendation
Does the SUI allow the users to report malicious behavior? (Pos)	Yes	No Recommendation

6.2 Findings and Comparison

The goal of this study was to compare the privacy scores obtained in the investigated systems. The comparison between the systems uses the common privacy scores since all the SUI have to answer the same number of assessment question (48 in the case of this study). The obtained reference common values in this test model are -27.38 for the flawed system and 30.73, as shown in table 6.5.

By comparing the results in table 6.3, it can be seen that both Diaspora and Twister have answered 40 questions as protecting the privacy and only 8 questions as risk generating, followed by Pump.io that has answered 30 privacy-protecting questions. Even though both Facebook and Gab have answered 19 questions as protecting privacy and 29 questions as risk generating, the difference between two systems is that GAP gives more access control over data in comparison with Facebook.

In the batch of non deployed systems, table 6.4 showed that Safebook (39 privacy-protecting questions), followed by Megaphone (38 privacy-protecting questions) and Garlanet (37 privacy-protecting questions) are the systems that ranked high in answering the privacy-protecting questions, while Cuckoo is the least of the non deployed systems to answer privacy-protecting questions. Fig. 6.1 and 6.2 compare the scores between PPS and PRS scores obtained respectively for deployed and non deployed systems.

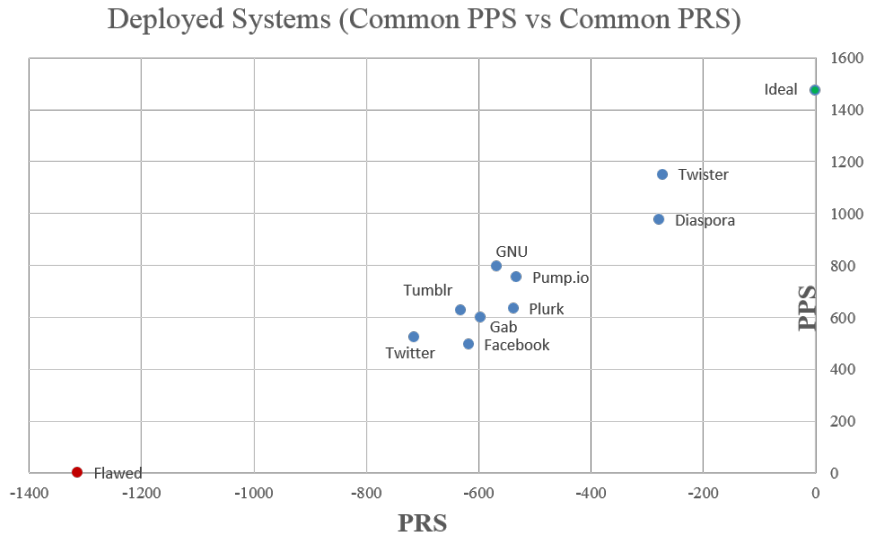


FIGURE 6.1: Comparison between common scores PPS and PRS for the deployed systems.

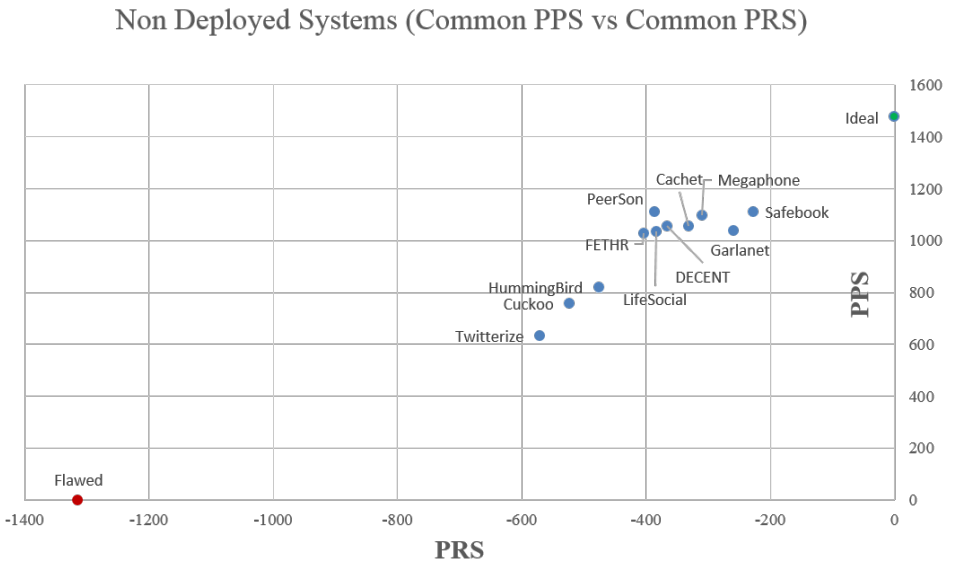


FIGURE 6.2: Comparison between common scores PPS and PRS for the non deployed systems.

Applying equation (5.4) and algorithm 1, we found that the overall common privacy score of Twitter is -4.00 (40% in comparison with the ideal system). It has the lowest score obtained in comparison with other systems in the deployed systems, followed by Facebook ($TPS = -2,54$, $TPS\_\% = 43\%$). While Twister obtained 18.31 (79% in comparison with the ideal system) and Diaspora obtained 14.56 (72% in comparison with the ideal system). Results showed as well that GAP and Tumblr got similar results 47% in comparison with the ideal system (refer to table 6.6 for more details).

The reason why Twitter got a lower privacy score comparing with Facebook is because of the access settings implemented for the users to control the visibility of their profiles, list of followers, and posts. For example, in Twitter, users cannot specify from whom to receive follow requests or change the visibility of the followers list contrary to Facebook. As for GAP, the developers claimed that they provide freedom of speech and thought, however, the platform has centralized architecture and the providers can access and administer the data of users. Fig. 6.3 shows a graphical representation of the different results obtained for the deployed system.

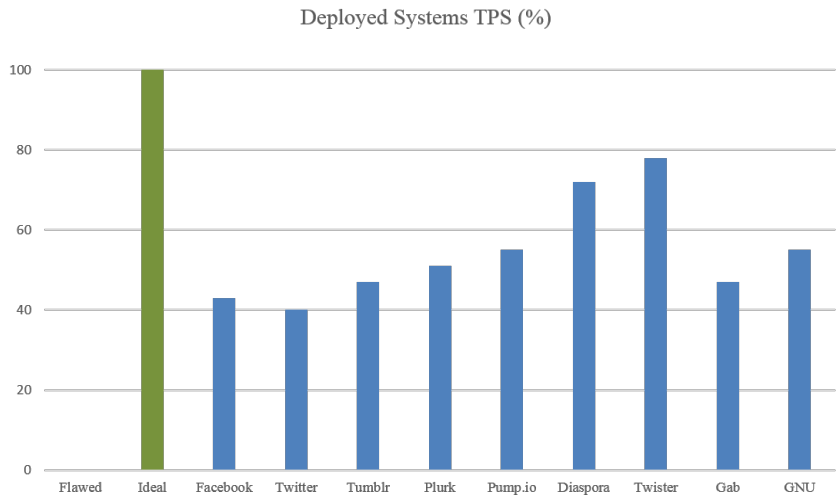


FIGURE 6.3: Comparison the deployed systems in terms of TPS (%).

For the non deployed systems, we found that in overall Safebook scored the highest in terms of overall privacy score ($TPS = 18.38, TPS\_\% = 79\%$), followed by Megaphone ($TPS = 16.38, TPS\_\% = 75\%$) and Garlanet ($TPS = 16.23, TPS\_\% = 75\%$). While Cuckoo obtained 4.88 (56% in comparison with the ideal system) and Twitterize obtained 1.29 (49% in comparison with the ideal system) (refer to table 6.7 for more details).

The reason why Twitterize got the lowest privacy score because it uses the same functionalities as Twitter and depends on Twitter for the storage of data. As for Cuckoo, the prototype was not built to protect the privacy of uses but to provide the users the similar functionalities of online social networks. Fig. 6.4 shows a graphical representation of the different results obtained for the non deployed system.

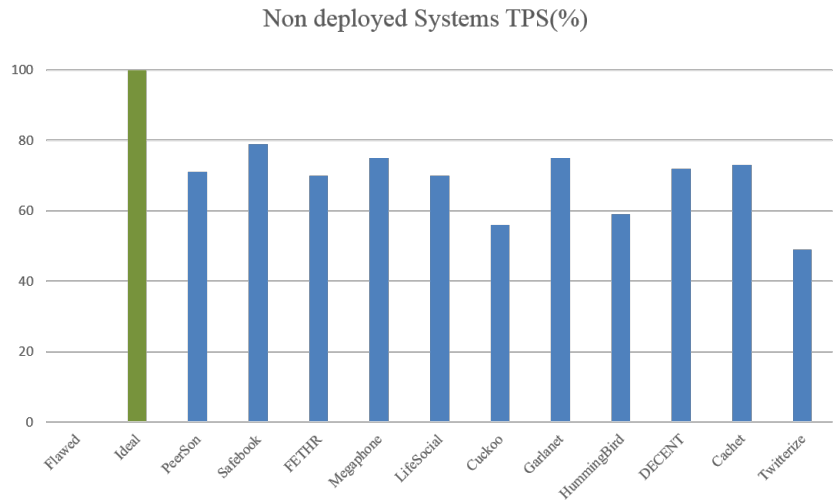


FIGURE 6.4: Comparison the non deployed systems in terms of TPS (%).

Specific privacy scores can not be used to compare different systems, but they can be used to compare between the privacy protection score PPS and privacy risk score PRS in each system. Fig. 6.5 and 6.6 compare the specific scores between PPS and PRS scores obtained respectively for deployed and non deployed systems.

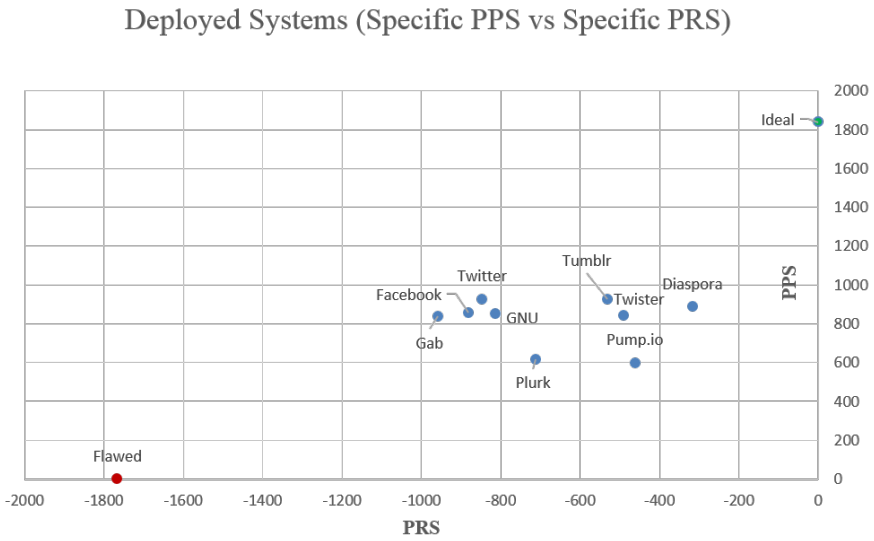


FIGURE 6.5: Comparison between specific scores PPS and PRS for the deployed systems.

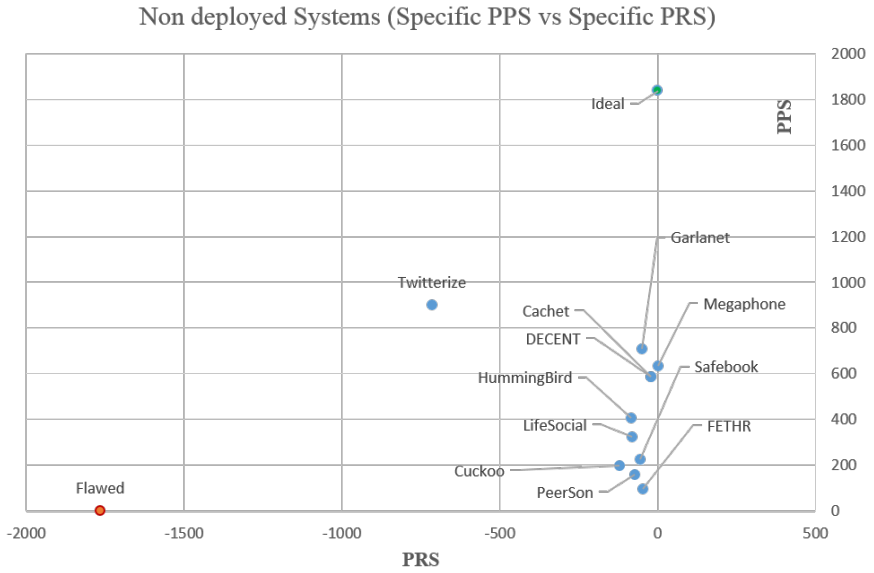


FIGURE 6.6: Comparison between specific scores PPS and PRS for the non deployed systems.

6.3 Discussion

One of the well-known processes to assess and evaluate privacy risk in systems is by conducting a privacy impact assessment (PIA). PIA is part of Privacy by Design [292] and it is proposed to identify and quantify privacy risks in a system and take decisions on whether and how to mitigate, transfer, or accept these privacy risks [285]. In 2018, PIAs become mandatory for companies under article 35 in GDPR [293] (called Data Protection Impact Assessment-DPIA). PIAs are important tools for accountability and to ensure compliance with the regulation.

The present framework methodology is similar to the methodology proposed by the French Data Protection Authority (CNIL) [294] to carry out PIA in the context of GDPR. The CNIL methodology is composed of 4 iterative steps: (1) study of the context to gain a clear overview of the data processing operations under consideration, (2) study of the fundamental principles and assessment of controls protecting data subjects' rights, (3) study of the risks related to the security of data (how much damage would be caused by all the potential impacts), and (4) validation of the PIA and decide whether or not to accept the results in light of the findings. However, the CNIL methodology differs from the proposed framework in many regards. The CNIL methodology is not specific to online social networks and it is intended for internal use only by system providers and data controllers, the results of the assessment are not shared with the end users but they are used to improve the implementation of privacy protection techniques and to demonstrate the compliance with laws and regulation. Moreover, it does not provide a privacy score and it considers only the calculation of potential privacy risks without considering the mechanisms implemented to protect the privacy in the system.

The proposed framework differs significantly from existing privacy scores and privacy assessment processes. As discussed in chapter 2, previous models computed privacy scores in OSNs based on the sensitivity and the visibility of users' attributes (such as profile's items, relationships,...). Our approach is related to these models, the formula proposed to calculate the $ScoreAQ$ is based on the visibility and we replaced the sensitivity by the impact of privacy and security as two additional factors in calculating privacy score, since the sensitivity is a property of the impact. Furthermore, the overall privacy score is not based only on the assessment risk available in the investigated system, but also on the privacy protection provided by the system to their users.

6.4 Summary

This chapter provided a means of evaluation for privacy scoring framework introduced in the previous chapter. We conducted an empirical study using the proposed information privacy metric to evaluate and compare between different online social networks divided into two categories: (i) 9 systems that are deployed and operational, and (ii) 11 systems that are proposals found in the literature. Our study revealed some interesting findings. In general, the non deployed systems in our dataset got higher scores than most of the deployed systems, this is expected since that the non deployed systems are prototypes built to mainly protect the privacy at the cost of providing functionalities that can attract users. Fig. 6.7 and 6.8 summarize the comparison between all systems (deployed and non-deployed systems), respectively, in terms of common PPS and PRS.

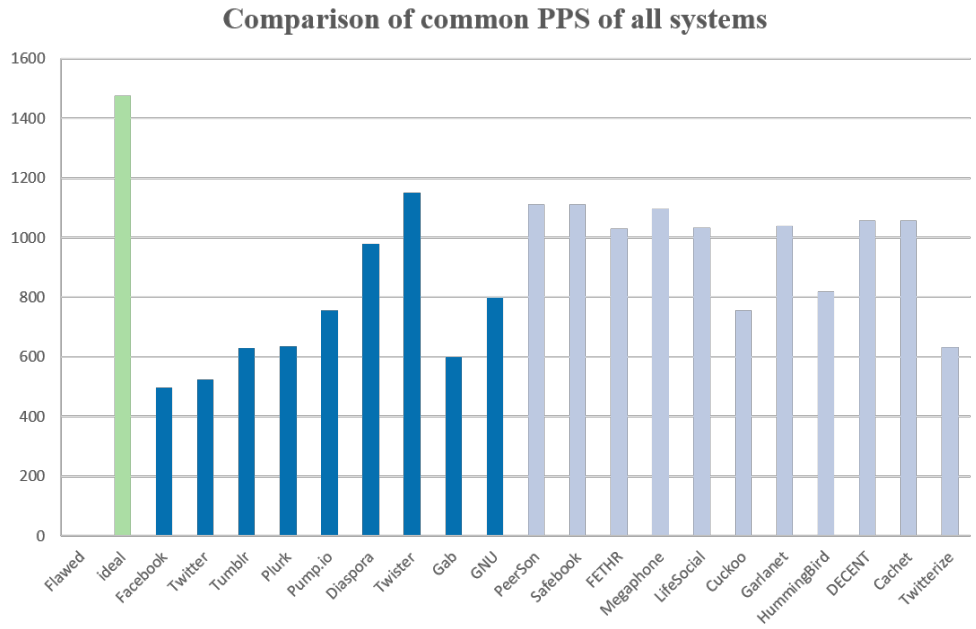


FIGURE 6.7: Comparison between common PPS for all systems.

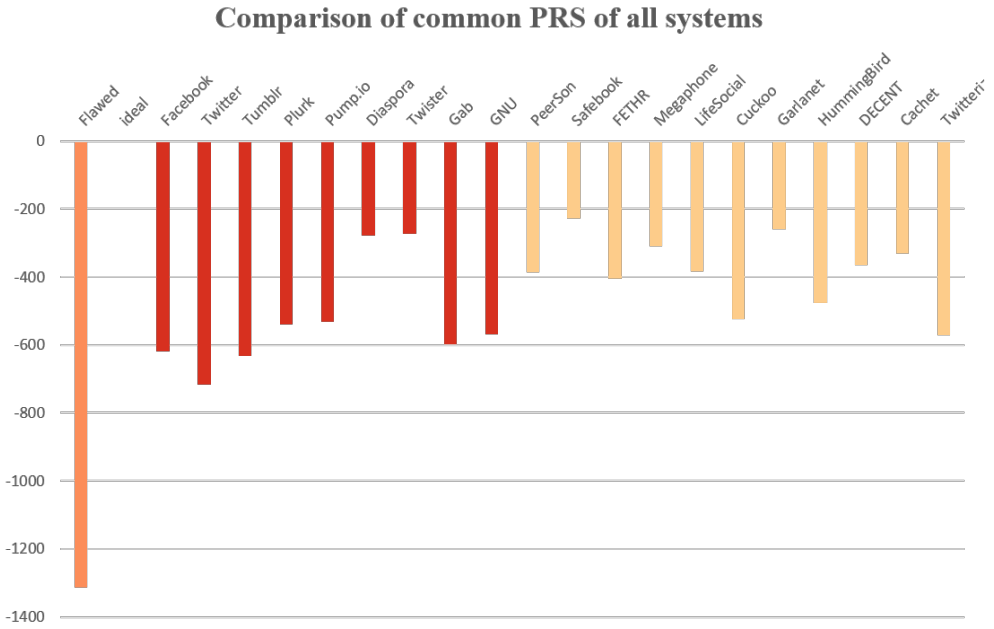


FIGURE 6.8: Comparison between common PRS for all systems.

While most of the deployed systems favor attracting users with more functionalities, especially that the services provided are free of charges and the user's data stored in the databases are used for monetary gain. Fig. 6.9 and 6.10 summarize the comparison between all systems (deployed and non-deployed systems), respectively, in terms of specific PPS and PRS.

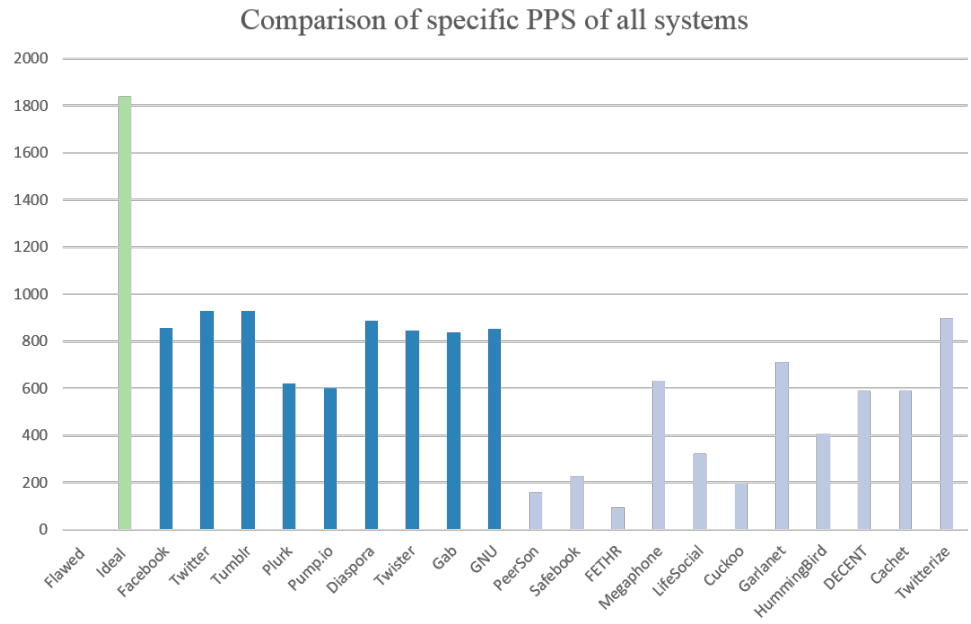


FIGURE 6.9: Comparison between specific PPS for all systems.

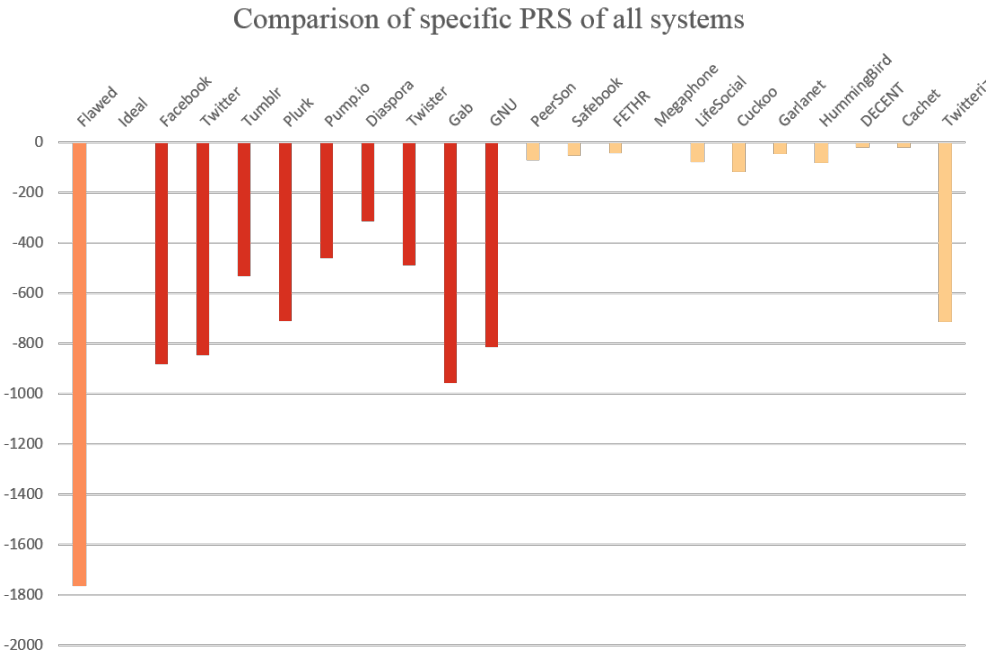


FIGURE 6.10: Comparison between specific PRS for all systems.

Overall, our information privacy assessment score demonstrates its feasibility of providing users with a simple-to-use tool to establish an overview of the level of information privacy of OSNs and compare privacy protections and risks between different systems. The obtained results showed the potential of the proposed framework. Additionally, the study contributes to the privacy scoring research field to understand more the inner functioning of OSNs. It shows also the importance of protecting the privacy and how it can be a challenge especially with the existing

trade-off between the necessity to make the platforms usable, friendly and easy to use and between the protection of the private life.

To the best of our knowledge, we are the first to present an algorithmic model that computes privacy score from this perspective and focuses on microblogging OSNs.

Chapter 7

Conclusion and Future Work

In the last past years, Online Social Networks (OSNs) have shifted the traditional paradigm of human interactions and communication into a digital representation of their relationships and daily activities. Ranging from blogging services to social communities, multimedia sharing, and virtual worlds, the demand on such online services grows continually. They supply services to a broad range of users of all ages, various social backgrounds, and users with limited technical skills.

Users enjoy sharing their activities and interests and connecting with friends using the services of OSNs. However, this advantage comes at the cost of privacy risks and data breaches. A large amount of personal information (sensitive or non-sensitive) is accessible to all the Internet. Moreover, advanced data analytics have made it easy to collect and aggregate data to reveal hidden information.

With the large number of threats and attacks on OSNs, privacy-oriented service providers and researchers have introduced new systems that offer online social functionalities and at the same time advocate for privacy protection. Some systems add a privacy layer while others are built using privacy by design methodologies.

With a multitude of privacy controls and techniques implemented in these new MOSNs, a necessity of tools to evaluate the privacy protection techniques in OSNs have appeared. Privacy scoring models are used to evaluate the effectiveness of the privacy level in OSNs. However, the challenge is how to measure and evaluate the privacy in OSNs since defining privacy itself is a challenging issue. Privacy is elusive and subjective because it is related to what people consider sensitive, i.e. which information each person wants to keep secret.

The present thesis proposes IPAM framework, an enhancing generic privacy scoring framework to quantify, assess, and evaluate privacy in OSNs, with a focus on microblogging systems.

This final chapter summarizes the key contributions and findings of the present thesis (Section 7.1) and outlines some guidelines for future work in Section 7.2.

7.1 Conclusions

In chapter 2, we introduced Microblogging Online Social Networks and illustrated their main stakeholders and the data types used in such systems. We defined privacy and its requirements and we discussed some known laws and regulations that govern information privacy. Furthermore, we identified and classified privacy threats and attacks that can be perpetrated in OSNs and we discussed some mitigation techniques and countermeasures to overcome these threats. Then we presented some existing privacy-specific measurement models in OSNs. The discussion revealed that the existing privacy scoring models in OSNs have some limitation to accurately calculate privacy scores:

- they evaluate privacy in OSNs from the user's perspective. They assess privacy based on the visibility and the sensitivity of the attributes from a user's profile.
- they consider the impact of the visibility of attributes to other users but not to the system provider.
- they do not consider the impact of security requirements in their evaluation.
- they are system-specific and cannot be used to compare privacy scores across different systems.

Before designing the framework, we conducted an online questionnaire survey to understand and analyze the attitude of users towards privacy in OSNs, as presented in Chapter 3. The survey was designed to answer two research questions of how users' information sharing behavior in OSNs is influenced and what are their preferences in terms of privacy in OSNs.

A sample of 542 participants was analyzed and the results reveal that 13% of the participants did not use any kind of OSNs, mostly for privacy concerns. The analysis of remaining 87% of the sample revealed that information sharing behavior can be influenced by 4 factors, namely: (1) privacy awareness, (2) control of information, (3) data collection limitation, and (4) granularity of privacy settings and functionalities. The study did not report any privacy paradox. The analysis also showed that age and gender do not have an influence on the behavior of users in terms of sharing information in OSNs. Women are more concerned and more aware of privacy issues in OSNs than men, but both tend to behave the same way in sharing information. Furthermore, users behave in the same manner when they are sharing their information either with friends or with strangers. Results also showed that users prefer to have a balance between functionalities and privacy protection.

The presented results can be explained by the protection motivation theory that argues that protection behavior is motivated by the perceived severity of a risk or a threatening event. In other words, users are inclined to share less information as a result of the privacy risks and threats present in OSNs, which defeats the main purpose of social networking to communicate with users and share information. Thus, protecting information privacy and implementing further privacy enhancing controls can attract more users to use OSNs. The results of Chapter 3 have been written in a paper entitled "Revisiting Privacy: Do We Really Care About Our Privacy in Online Social Networks?" and submitted to the journal *Behaviour & Information Technology* (currently under review).

Furthermore, this thesis conducted an extensive state-of-the-art of the existing microblogging and social network systems in chapter 4. In line with the mitigation approaches and privacy principles discussed in chapter 2, we identified a set of 7 criteria to compare 24 different OSN systems divided into two categories: (i) 12 systems that are/were deployed and operational, and (ii) 12 systems that are proposals found in the literature. As each system has its own features and characteristics, we chose generic and common items to OSNs. We introduced the service provided by the systems, the design architecture, the storage mechanisms, the encryption algorithms, the security goals, the privacy settings and controls implemented in each system, and the functionalities provided. Furthermore, we presented a comparative evaluation of the surveyed OSN systems based on the security and privacy violations and mitigation techniques implemented. The comparative study showed that most of the systems are about meeting the privacy principles in order to be in compliance with the applicable laws and regulation (e.g. EUGDPR). Also, most of the

systems provide privacy settings (differ from a system to another) and privacy policies. They implemented some kind of encryption, either TLS certificate, public-key, or symmetric cryptography. Furthermore, some solutions eliminated the central system provider and opted for decentralized systems where the users can choose where to store the data. The results of Chapter 4 have been written in a paper entitled "Privacy Analysis on Microblogging Online Social Networks: A Survey" and published in the journal *ACM Survey Computing*.

In chapter 5, we presented information privacy assessment metric (IPAM). IPAM is a novel generic framework to compute the privacy score in microblogging Online Social Networks. The framework helps (i) to guide the development of privacy metrics and (ii) to measure and assess the privacy level of OSNs, more specifically microblogging systems. The proposed methodology is based on the Plan-Do-Study-Act (PDSA) cycle and the proposed algorithmic model to compute privacy scores is based on the Goal-Question-Metric (GQM) paradigm. The information privacy scores are calculated from the impact of privacy and security requirements, accessibility, and extraction difficulty of information in MOSNs. The privacy scores computed using the framework are intended to help the end users to understand the potential impact of microblogging OSNs on their privacy. System providers can also use the results of the framework to implement the privacy recommendations provided by the framework and strengthen the position of their systems in the market.

The proposed framework differs from existing privacy scores in OSNs and privacy impact assessment processes. Existing proposed models calculated the privacy score based on the sensitivity of profiles' attributes and their visibility to other users, without considering the risks generated from systems providers and the functionalities provided. An overview of the IPAM framework have been presented in a workshop paper entitled "Privacy in Microblogging Online Social Networks: Issues and Metrics" presented in XV RECSI workshop. A detailed version of the results have been written in a paper entitled "IPAM: Information Privacy Assessment Metric in Microblogging Online Social Networks" and published in the journal *IEEE Access*.

In chapter 6, we analyzed and evaluated the feasibility of the proposed framework. We compared the privacy scores obtained from using the algorithmic model for the systems surveyed in chapter 4. The obtained results show the potential of the proposed framework and revealed some interesting findings. In both deployed and non deployed sets, Twitter got the lowest privacy scores, followed by Facebook. While Safebook, from the non deployed set, got the highest score. This is expected since the non deployed systems are prototypes built in the purpose of preserving privacy in online social networks. Part of this study was reported in the article "IPAM: Information Privacy Assessment Metric in Microblogging Online Social Networks" published in the journal *IEEE Access*.

This work represents the first steps towards developing a practical framework to quantify privacy in microblogging systems using the impact of privacy and security requirements, accessibility, and extraction difficulty of information in MOSNs. The prototypical study of the information privacy metric illustrated its utility to obtain an easy-to-use overview of the information privacy score in microblogging OSNs and compare information privacy risk factors between different systems. The framework will increase the transparency of information privacy protection and will empower end users to make better decisions about selecting and using OSNs.

To the best of our knowledge, we are the first to present an algorithmic model that computes privacy score from this perspective and focuses on microblogging OSNs.

7.2 Future Work

Future research can make use of our framework to develop tools to further enhance the assessment of information privacy in Online Social Networks.

In relation to the studied online questionnaire survey, cross-cultural research is recommended to compare and investigate further the impact of different cultures on the perception of privacy on OSNs, also a study about the effect of education on information sharing behavior and on privacy concerns should be investigated.

In relation to the proposed framework, future research can focus on automating the extraction of values and answers of assessment questions for the parameters that our framework uses to compute privacy scores. The automatic analysis of different sources like user feedback, risk assessment reports, research surveys, event loggers, etc. can be used as input for the framework. The extraction of the online social network's structure, business processes, assets and services, security boundaries, and implemented controls will be automatically generated.

Also, to further evaluate the feasibility future research can focus on extending the evaluation of the results by running usability tests and surveying real users of microblogging systems. This evaluation can be used to test the utility of the proposed framework to end users and to validate the results obtained from applying the privacy metric.

Furthermore, the proposed privacy score metric can be converted to an API to be integrated into the internal functioning of OSN systems. The incorporation of the information privacy score by system providers can give end users insurance about the privacy controls and mechanisms implemented in the system. Additionally, the privacy score can be used as part of the Data Privacy Assessment (DPIA) in compliance with article 35 of GDPR.

The information privacy assessment metric can be complemented with a graphical user interface to enable easy use of the metric and an accessible platform to compare the privacy scores of multiple OSNs. With the graphical user interface, users can get a fast overview of privacy protection and risks in a system and make a quick decision about selecting an OSN.

In addition, future research can generalize the use of the proposed methodology and information privacy metric to other types of OSNs, for example, photo and video sharing or business networking systems. Another generalization can be for online systems other than Online social networks, like evaluating and assessing privacy level for e-health or financial applications.

Appendix A

Survey Questionnaire

A.1 Information Sharing Behavior (ISB)

1. Please, indicate how sensitive the following items to you from 1 (not sensitive) to 5 (extremely sensitive):
    - Name
    - Surname
    - Username
    - National Identifying Number
    - Age
    - Birth date
    - Gender
    - Avatar or profile image
    - Civil Status
    - Phone Number
    - Email address
    - Postal address
    - Personal interests and preferences
    - Profession or Education
    - Political affiliation
    - Religion affiliation
    - Sexual orientation
2. Please indicate how sensitive the following items that you can share about you from 1 (not sensitive) to 5 (extremely sensitive):
    - Lifestyle information (personal photos, post history, personal details as your love life, location, etc.)
    - Curriculum vitae information (languages . . .)
    - Work – profession related information
    - Religious beliefs
    - Political information
    - Business information
    - Health related information

- Financial information or consumption habits (what things do you buy, where do you buy them, etc.)
- Casual information (food, restaurants, sports, cars, etc.)
- Sensational information (news, location, etc.)

3. Please indicate how sensitive you consider each type of information shared on OSN's groups from 1 (not sensitive) to 5 (extremely sensitive):
   - Lifestyle information (personal photos, post history, personal details as your love life, location, etc.)
   - Curriculum vitae information (languages ...)
   - Work – profession related information
   - Religious beliefs
   - Political information
   - Business information
   - Health related information
   - Financial information or consumption habits (what things do you buy, where do you buy them, etc.)
   - Casual information (food, restaurants, sports, cars, etc.)
   - Sensational information (news, location, etc.)

A.2 Perceived Privacy Awareness (PPA)

1. Are you aware of the privacy threats present in OSNs?
2. Do you worry about your personal data (videos, photos, audios,...) to be accessed by other users or third parties without your consent?

A.3 Perceived Control of Information (PCI)

1. To register in a OSN, I prefer using:
   - My personal data as name, age, gender, etc.
   - My email address
   - Random identification generated by the system
   - Free access: No identification required
2. I prefer that the OSN offers me the possibility to sign up:
   - Only with my real name
   - I can choose between my real name or a pseudonym
   - Only with a pseudonym
3. To access my account in the OSN, I prefer the password to be:
   - The same password that I use in other sites
   - A unique password, but short and easy to remember.

- A unique password but at least 10 characters (numbers, letters and symbols) in length
- When possible I use an authentication based on a double factor such as password and mobile number

4. Please indicate your preference for the following items:

   - My identity (name, age, gender...)
   - My profile
   - My friendship list
   - My posts (messages, images, videos...)
   - What other users post about me
   - Groups I create
   - Groups I am subscribed to
   - The posts I share in groups
   -

5. I prefer that the membership list of the groups I am subscribed in to be:

   - Visible to all the users of the OSN and Internet
   - Only visible to group members
   - Not visible at all

6. I prefer to subscribe to groups where:

   - Only the group administrator can add users
   - The group administrator and the chosen users by the administrator can add users
   - Any user of the group can add users

7. Please evaluate the importance of the following actions from 1 (not important) to 5 (very important) :

   - Rectify published content
   - Remove published content
   - Erase published content
   - Change who can access to the published content

A.4 Data Collection Limitation (DCL)

1. Do you know what kind of data is collected in the OSN you use and why it is collected for?

2. Regarding the data usage collected by the service provider, to what extent do you agree or disagree with the statements shown below?

   - The OSN should clearly inform the user about the data collected usage
   - Users should decide the use that will be given to the data collected by the OSN

- Users should have the ability to choose which data to share with the OSN
- The OSN should clearly inform the user about the data that will be collected

3. Please indicate how sensitive you consider each kind of data collected from 1 (not sensitive) to 5 (extremely sensitive):

   - Information that you provide like name, etc...
   - Things that you do on the OSN (posting, ...)
   - Information about your network- connections
   - Information about access devices to OSN
   - Location information

A.5 Policies Understanding (PU)

1. Do you read the terms and conditions before creating an account in an OSN?
2. Do you understand these policies?
3. Do you always agree to the term and conditions presented by the OSN?

A.6 Privacy Functionalities and Granularity (PFG)

1. Please rate how important the following functionalities are to you in an OSN from 1 (not important) to 5 (extremely important):

   - Create profiles
   - Set the visibility of my profile (who can see it)
   - Set my personal interests like news, music section...
   - Modify my profiles
   - Delete my account
   - Accept or reject friendship requests
   - Set the visibility of my friendship list (who can see it)
   - Search other users
   - Set with whom I want to share the content I post
   - Share or resend posts
   - Share multimedia data (images, videos, audio ...)
   - Mention other users on comments
   - Comment on other users' posts
   - Be able to see where I am mentioned
   - Recommend content, places or users
   - Chat with my friends

2. Are the privacy settings offered by the OSN easy to use?
3. Do you feel that the privacy settings provided by the OSN are enough to protect your privacy?

4. Please indicate how important you consider the following privacy settings from 1 (not important) to 5 (extremely important):

    - Profile visibility settings
    - Share content visibility settings
    - Settings about information related with me
    - Set the control on how others can find you
    - Limit who can send friendship requests

Appendix B

Supplementary Materials for Chapter 3

B.1 Users Preferences for Profile Management

TABLE B.1: How do users prefer to register to the OSN services

	Freq.	**%**
My personal data as name, age, gender, etc.	68	14%
My email address	282	60%
Random identification generated by the system	68	14%
Free access: No identification required	52	11%

TABLE B.2: How do users prefer to log in to the OSN services

	Freq..	**%**
Only with my real name	70	15%
I can choose between my real name or a pseudonym	355	76%
Only with a pseudonym	45	10%

TABLE B.3: Users password's preferences in OSNs

	Freq.	**%**
The same password that I use in other sites	121	26%
A unique password, but short and easy to remember.	89	19%
A unique password but at least 10 characters (numbers, letters and symbols) in length	158	34%
When possible I use an authentication based on a double factor such as password and mobile number	102	22%

TABLE B.4: Profile items requirement

	Name		**Surname**		**Username**		**SSN**		**Age**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Required	242	51%	147	31%	404	86%	33	7%	119	25%
Optional	228	49%	323	69%	66	14%	437	93%	351	75%
	Birthdate		**Gender**		**Avatar**		**Civil status**		**Phone Nº**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Required	97	21%	110	23%	128	27%	8	2%	21	4%
Optional	373	79%	360	77%	342	73%	462	98%	449	96%
	Email@		**Postal@**		**Interests**		**Education**		**Political affil**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Required	277	59%	7	1%	47	10%	35	7%	2	0%
Optional	193	41%	463	99%	423	90%	435	93%	468	100%
	Religion affil		**Sexual affil**							
	Freq.	**%**	**Freq.**	**%**						
Required	2	0%	4	1%						
Optional	468	100%	466	99%						

TABLE B.5: Profile items sensitivity

	Name		**Surname**		**Username**		**SSN**		**Age**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sens.	105	22%	34	7%	261	56%	10	2%	78	17%
Not that sens.	90	19%	79	17%	98	21%	10	2%	114	24%
Sensitive	134	29%	112	24%	74	16%	34	7%	159	34%
Very sens.	68	14%	112	24%	19	4%	48	10%	69	15%
Extremely sens.	73	16%	133	28%	18	4%	368	78%	50	11%
	Birthdate		**Gender**		**Avatar**		**Civil status**		**Phone Nº**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sens.	47	10%	114	24%	134	29%	84	18%	12	3%
Not that sens.	103	22%	103	22%	88	19%	82	17%	14	3%
Sensitive	139	30%	129	27%	133	28%	134	29%	35	7%
Very sens.	90	19%	58	12%	62	13%	71	15%	65	14%
Extremely sens.	91	19%	66	14%	53	11%	99	21%	344	73%
	Email@		**Postal@**		**Interests**		**Education**		**Political affil**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sens.	36	8%	19	4%	66	14%	37	8%	51	11%
Not that sens.	62	13%	27	6%	95	20%	79	17%	93	20%
Sensitive	130	28%	39	8%	154	33%	141	30%	137	29%
Very sens.	108	23%	72	15%	76	16%	102	22%	99	21%
Extremely sens.	134	29%	313	67%	79	17%	92	20%	90	19%
	Religion affil		**Sexual affil**							
	Freq.	**%**	**Freq.**	**%**						
Not sens.	35	7%	45	10%						
Not that sens.	42	9%	40	9%						
Sensitive	83	18%	85	18%						
Very sens.	86	18%	75	16%						
Extremely sens.	224	48%	225	48%						

B.2 Users Preferences for Message Management

TABLE B.6: Post Sensitivity

	Personal info		**CV info**		**Work-related**		**Religion**		**General Info**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sensitive	7	1%	18	4%	20	4%	40	9%	55	12%
Not much sensitive	23	5%	58	12%	60	13%	54	12%	112	24%
Sensitive	84	18%	135	29%	137	29%	85	18%	145	31%
Very sensitive	122	26%	107	23%	115	25%	88	19%	74	16%
Extremely sensitive	233	50%	150	32%	136	29%	199	43%	80	17%
	Politics		**Business**		**Health**		**Financial info**			
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**		
Not sensitive	30	6%	26	6%	11	2%	9	2%		
Not much sensitive	52	11%	68	15%	32	7%	26	6%		
Sensitive	91	19%	122	26%	56	12%	52	11%		
Very sensitive	84	18%	107	23%	91	19%	96	21%		
Extremely sensitive	210	45%	144	31%	278	59%	285	61%		

B.3 Users Preferences for Group Management

TABLE B.7: Group subscription

	Freq.	**%**
Only the group administrator can add users	186	40%
The group administrator and the chosen users by the administrator can add users	240	51%
Any user of the group can add users	44	9%

TABLE B.8: Group membership list visibility

	Freq.	**%**
Visible to all the users of the OSN and Internet	24	5%
Only visible to group members	377	80%
Not visible at all	69	15%
	470	100%

TABLE B.9: Group message sensitivity

	Personal info		**CV info**		**Work-related**		**Religion**		**General Info**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sensitive	11	2%	20	4%	26	6%	42	9%	70	15%
Not much sensitive	36	8%	59	13%	67	14%	50	11%	110	23%
Sensitive	99	21%	142	30%	131	28%	93	20%	135	29%
Very sensitive	99	21%	98	21%	107	23%	85	18%	79	17%
Extremely sensitive	225	48%	151	32%	139	30%	200	43%	76	16%
	Politics		**Business**		**Health**		**Financial info**			
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**		
Not sensitive	31	7%	27	6%	13	3%	16	3%		
Not much sensitive	55	12%	66	14%	37	8%	32	7%		
Sensitive	93	20%	131	28%	73	16%	71	15%		
Very sensitive	85	18%	97	21%	94	20%	105	22%		
Extremely sensitive	206	44%	149	32%	253	54%	246	52%		

B.4 Users Preferences for Privacy Settings

TABLE B.10: Easy usage of Privacy settings

	Freq.	**%**
Yes, they are pretty easy to use	189	40%
Partially, I find them a bit difficult to use	210	45%
No, they are not easy to use	71	15%

TABLE B.11: Privacy settings are they enough to protect privacy?

	Freq.	**%**
Yes, they completely protect my private life	17	4%
Partially, but they can be more fine-grained to protect me more	321	68%
No, they don't protect me at all	132	28%

TABLE B.12: Privacy settings importance

	Profile Vis		**Content Vis**		**Personal Info**		**Control Search**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not important	6	1%	5	1%	3	1%	6	1%
Somewhat important	22	5%	13	3%	10	2%	22	5%
Important	73	16%	87	19%	49	10%	92	20%
Very important	127	27%	135	29%	97	21%	120	26%
Extremely important	242	51%	230	49%	311	66%	230	49%

B.5 Users Preferences for Data Collection

TABLE B.13: Data collection knowledge

	Freq.	**%**
Yes, I have been informed clearly of the data collected and its usage	68	14%
Partially, I know what kind of data is collected but I don't know what it will be used for	261	56%
No, I don't know what data is collected or what its usage is	141	30%

TABLE B.14: Data collected sensitivity

	Personal Info		**Shared Contents**		**Connections**		**Traffic data**		**Location**	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Not sensitive	10	2%	10	2%	8	2%	10	2%	5	1%
Not much sensitive	26	6%	39	8%	31	7%	35	7%	10	2%
Sensitive	48	10%	131	28%	96	20%	96	20%	38	8%
Very sensitive	68	14%	148	31%	144	31%	121	26%	60	13%
Extremely sensitive	318	68%	142	30%	191	41%	208	44%	357	76%

Appendix C

Assessment Questions

C.1 Common Set

- **Profile**
  1. Can the unregistered users access the service without creating a profile?
  2. Are the following items required to create a profile?
     - Name
     - Surname
     - Username
     - National Identifying Number
     - Age
     - Birth date
     - Gender
     - Avatar or profile image
     - Civil Status
     - Phone Number
     - Email address
     - Postal address
     - Personal interests and preferences
     - Profession or Education
     - Political affiliation
     - Religious affiliation
     - Sexual orientation
     - Contact information
  3. Is it required to be authenticated to access the services?
  4. Can the users create multiple profiles with the same credentials?
  5. Once the profile is created, is it public by default?
  6. Can the user change the visibility of the profile?
  7. Can the user edit the items in the profile?
  8. Can the user delete the profiles?
  9. Can the SUI edit the user information without consent?
  10. Can the SUI delete profiles without the consent of their owners?
- **Relationships**

11. Are the friendship requests accepted automatically without consent?
12. Can the users accept a friendship request?
13. Can the users deny a friendship request?
14. Can the user restrict from whom to receive friendship requests?
15. Is the relationship list public by default?
16. Can the user change the visibility of the relationship list?
17. Can the user delete friends from the friendship list?

- **Posts**

18. Is a new post visible to public by default on the user's timeline?
19. Can the users specify the audience of a new post?
20. Can the users edit their posts?
21. Can the users delete their posts?
22. Can the SUI edit user's data without consent?
23. Can the SUI delete user's data without consent?

- **Data Storage**

  - **Option 1.**
    24. Is data stored in centralized databases handled by the SUI?
    25. Does the SUI replicate the data stored?
    26. Does the SUI provider have a secondary site for data storage?
    27. Does the SUI delete the data stored once the users delete it?
  - **Option 2.**
    24. Is data stored in pods or clients' machines?
    25. Does the SUI duplicate and store the data stored in the pods?
    26. Is the data replicated?
    27. Can the SUI delete the data stored without consent?
  - **Option 3.**
    24. Is data stored in Hybrid servers?
    25. Does the SUI handle the storage of the data of users?
    26. Is the data replicated?
    27. Can the SUI delete the data stored without consent?

- **Data Collection**

28. Does the SUI collect data from users? (If yes, go to Specific AQs)
29. Does the SUI analyze and sell data? (If yes, go to Specific AQs)

- **Data Encryption**

30. Is the data stored encrypted? (If yes, go to Specific AQs)
31. Are the encrypted communication channel used when transferring data? (If yes, go to Specific AQs)

C.2 Specific Set

- **Profile**

1. Can the users reset their authentication?
2. Can the users recover their authentication?
3. Does the SUI enforce a limit of consecutive invalid login attempts by a user during a period of time?
4. Does the SUI send alerts for unknown logins?
5. Can the users deactivate their profiles without deleting them?

- **Posts**

6. Does the SUI add location information by default to the posts?
7. If yes, can the users deactivate the option of location information?

- **Groups**

8. Is the group once created visible to all by default?
9. Can the group administration restrict the visibility of the group?
10. Can the users be added to a group without their consent?
11. Can anyone add users to the group?
12. Can anyone delete users to the group?
13. Is the membership list public by default in the group?
14. Can the group administrator control the visibility of the membership list?
15. Can the users quit a group?
16. Can SUI delete a group without the consent of its owner?

- **Data Collection**

  – Does the SUI collect data from users? (if yes continue) (Not counted)

17. Does the SUI explain the data collected, what type and what for?
18. Does the SUI ask for users' consent to collect data?
19. Can the users withdraw their consent?
20. Does the user control the data to be collected by the SUI?

  – Does the SUI analyze and sell data? (if yes continue) (Not counted)

21. Does the SUI ask users' permission to analyze and sell the data?
22. Does the SUI use anonymization mechanisms before publishing data?
23. Does the SUI specify to whom the data are sold?
24. Can the users specify to whom the data will be sold?

- **Data Encryption**

  – Is the data stored encrypted? (if yes continue) (Not counted)

25. Is the encryption algorithm used weak?
26. Are the key lengths weak?
27. Does the SUI generate the keys?
28. Are the keys stored in the SUI?

Are the encrypted communication channel used when transferring data? (if yes continue) (Not counted)

29. Does the SUI use weak protocols for SSL/TLS?
30. Does the SUI use weak key length for SSL/TLS?

- **Functionalities**

31. Can the users post messages on others' timelines (non friends)?
32. Can the user control who can post a message in their timeline?
33. Can the users mention/tag any other user (non friends) in the comments?
34. Can the user control who can mention them in the comments?
35. Can the users share or resend friends' posts?
36. Can the users share or resend any other user's posts?
37. Can the users comment on any other users' posts?
38. Can the users receive direct messages from anyone?
39. Can the users restrict from whom to receive a DM?
40. Does the SUI provide users with updates, news and advertisement contents based on their behavior and interests?
41. Is yes, can the users accept or refuse to receive updates, news and advertisement contents?
42. Can the users search other users by identifier (name, email,...)?
43. If yes, can the users control who can search for them by identifier?
44. If yes, can the users control who can search for them by email?
45. Can the users search other users by interest?
46. Does the SUI detect the user's location?
47. Does the SUI recommend potential friends?
48. Does the SUI recommend potential interests?

- **Architecture and Application**

49. Does the SUI keep up to date all the appliances/ Software/ Hardware on a continual basis?
50. Does the SUI perform regular vulnerability assessments?
51. Does the SUI use layered protections?
52. Does the SUI provider use the security best practices in developing their applications?
53. Does the SUI developer update and patch regularly the application?
54. Does the SUI developer review and test the application for security vulnerabilities?

- **Settings**

  55. Does the SUI allow the users to adjust their privacy settings?
  56. Does the SUI provide automated privacy settings that learns from the user's behavior and preferences?
  57. Are the settings clear and easy to use?

- **Privacy Policies**

  58. Does the SUI provide privacy policies?
  59. Is yes, does the SUI inform the users about changes in the privacy policies?
  60. Are the privacy policies written in clear and understandable terms?
  61. Does the SUI update the policies regularly?

- **Feedback**

  62. Does the SUI implement user's feedback about the usability of privacy settings?
  63. Does the SUI allow the users to report malicious behavior ?
  64. Does the SUI allow the users to report compromised accounts or malicious users ?

- **API and third party relationships**

  65. Does the SUI developer use trusted external libraries?
  66. Does the SUI provide an API for developers to integrate the OSN services in their apps?
  67. Does the SUI allow third party applications to access and collect data?
  68. Does the SUI allow users to ban a third party application from accessing their information?

Appendix D

Assessment Questions Scores Score_AQ

D.1 Common Set

TABLE D.1: Common score for the reference systems

AQs	Flawed system	Ideal System	AQs	Flawed system	Ideal System
Profile			**Posts**		
AQ1	-44	44	AQ18	-38	38
AQ2			AQ19	-38	38
Name	-15	15	AQ20	-44	44
Surname	-16	16	AQ21	-44	44
Username	-13	13	AQ22	-23	38
SSN	-16	16	AQ23	-23	38
Age	-13	13	**Data storage**	**Option 1**	**Option 2**
Birthdate	-13	13	AQ24	-30	56
Gender	-13	13	AQ25	-32	56
Avatar	-15	15	AQ26	-20	49
Civil Status	-15	15	AQ27	-30	64
Phone Nº	-15	15	**Data collection**		
Email	-15	15	AQ28	-32	32
Postal	-16	16	AQ29	-32	32
Interests	-13	13	**Data encryption**		
Profession	-13	13	AQ30	-69	69
Politics	-16	16	AQ31	-44	44
Religion	-16	16			
Sexual Pref	-16	16			
Contact	-15	15			
AQ3	-69	69			
AQ4	-64	64			
AQ5	-38	38			
AQ6	-38	38			
AQ7	-18	18			
AQ8	-18	18			
AQ9	-13	22			
AQ10	-13	22			
Relationships					
AQ11	-38	38			
AQ12	-38	38			
AQ13	-32	32			
AQ14	-27	27			
AQ15	-38	38			
AQ16	-38	38			
AQ17	-25	25			

TABLE D.2: Common score for the deployed systems

AQs	Facebook	Twitter	Tumblr	Plurk	Pump.io	Diaspora	Twister	Gab	GNU
Profile									
AQ1	-44	-44	-44	6	6	3	44	-44	-44
AQ2									
Name	-15	-15	15	15	15	15	15	-15	-15
Surname	-16	-16	16	16	16	16	16	-16	-16
Username	1	1	1	2	2	4	7	1	1
SSN	16	16	16	16	16	16	16	16	16
Age	-13	13	-8	13	13	13	13	13	13
Birthdate	-13	-13	13	-13	13	13	13	13	13
Gender	-13	13	13	-13	13	13	13	13	13
Avatar	-15	-15	15	15	-12	15	15	15	15
Civil Status	-6	15	15	-15	15	15	15	15	15
Phone Nº	-15	-15	-15	15	15	15	15	15	15
Email	1	1	1	1	2	4	15	15	15
Postal	-7	16	16	-16	-13	16	16	16	16
Interests	-5	13	-13	-13	-10	13	13	-13	-13
Profession	-13	13	13	13	13	13	13	13	13
Politics	-7	16	16	16	16	16	16	16	16
Religion	-7	16	16	16	16	16	16	16	16
Sexual PRef	-7	16	16	16	16	16	16	16	16
Contact	-6	15	15	15	15	15	15	15	15
AQ3	69	69	69	69	69	69	69	69	69
AQ4	64	64	64	64	-64	64	64	64	-64
AQ5	-38	-38	-38	-38	30	-20	10	-38	-38
AQ6	-38	20	-38	10	20	30	-38	10	20
AQ7	18	18	18	18	18	18	18	18	18
AQ8	18	-18	18	18	-18	18	-18	18	18

AQs	Facebook	Twitter	Tumblr	Plurk	Pump.io	Diaspora	Twister	Gab	GNU
AQ9	-13	-13	-13	-13	-13	22	22	5	22
AQ10	-13	-13	-13	-13	-13	22	22	-13	22
Relationships									
AQ11	38	-38	-38	38	-38	-38	-38	-38	-38
AQ12	38	38	-38	38	-38	-38	-38	-38	38
AQ13	32	32	-32	32	-32	-32	-32	-32	32
AQ14	4	-18	-27	-27	-27	-27	-27	-27	-27
AQ15	-38	-38	-38	-38	-38	3	38	-38	-38
AQ16	5	-38	38	-38	-38	3	-38	10	-38
AQ17	25	-25	25	-25	-25	25	25	25	25
Posts									
AQ18	-38	-38	-38	-38	30	30	30	-38	-38
AQ19	5	-38	38	10	30	30	30	-38	20
AQ20	44	-44	44	44	44	44	-44	44	-44
AQ21	44	44	44	44	44	44	44	44	44
AQ22	-23	-23	-23	-23	-23	8	38	-23	38
AQ23	-23	-23	-23	-23	-23	-23	38	-23	-23
Data storage	**Option 1**	**Option 1**	**Option 1**	**Option 1**	**Option 2**	**Option 2**	**Option 2**	**Option 1**	**Option 2**
AQ24	-30	-30	-30	-30	56	56	56	-30	12
AQ25	11	11	11	11	56	56	56	11	56
AQ26	20	20	20	20	49	49	49	20	49
AQ27	-30	-30	-30	-30	-39	64	64	10	64
Data collection									
AQ28	-32	-32	-32	-32	32	-32	32	-32	-32
AQ29	-32	-32	-32	-32	32	32	32	-32	-32
Data encryption									
AQ30	-69	-69	-69	-69	-69	-69	69	-69	-69
AQ31	44	44	44	44	44	44	44	44	44

TABLE D.3: Common score for the non deployed systems

AQs	PeerSon	Safebook	FETHR	Megaphone	LifeSocial	Cuckoo	Garlanet	HummingBird	DECENT	Cachet	Twitterize
Profile											
AQ1	44	44	44	44	44	44	44	44	44	44	-44
AQ2											
Name	15	15	15	15	15	15	15	15	15	15	-15
Surname	16	16	16	16	16	16	16	16	16	16	-16
Username	-1	5	1	7	-1	5	7	1	-1	-1	1
SSN	16	16	16	16	16	16	16	16	16	16	16
Age	13	13	13	13	13	13	13	13	13	13	13
Birthdate	13	13	13	13	13	13	13	13	13	13	-13
Gender	13	13	13	13	13	13	13	13	13	13	13
Avatar	15	15	15	15	-10	15	15	15	15	15	-15
Civil Status	15	15	15	15	15	15	15	15	15	15	15
Phone Nº	15	15	15	15	15	15	15	15	15	15	-15
Email	1	-1	-1	-1	-1	-1	15	-1	-1	-1	1
Postal	16	16	16	16	16	16	16	16	16	16	16
Interests	13	13	13	13	13	13	13	13	13	13	13
Profession	13	13	13	13	13	13	13	13	13	13	13
Politics	16	16	16	16	16	16	16	16	16	16	16
Religion	16	16	16	16	16	16	16	16	16	16	16
Sexual Pref	16	16	16	16	16	16	16	16	16	16	16
Contact	15	15	15	15	15	15	15	15	15	15	15
AQ3	-69	69	-69	-69	-69	-69	69	69	-69	-69	69
AQ4	64	64	64	64	64	64	64	64	64	64	64
AQ5	-38	10	-38	-20	20	-38	20	-38	-25	-25	-38
AQ6	-38	15	-38	-38	-38	-38	-3	-20	-38	-38	20
AQ7	-18	-18	-18	-18	-18	-18	18	-18	-18	-18	18
AQ8	-18	-18	-18	-18	-18	-18	-18	-18	-18	-18	-18

AQs	PeerSon	Safebook	FETHR	Megaphone	LifeSocial	Cuckoo	Garlanet	HummingBird	DECENT	Cachet	Twitterize
AQ9	22	22	22	22	22	-13	22	-13	22	22	-13
AQ10	22	22	22	22	22	-13	22	-13	22	22	-13
Relationships											
AQ11	38	38	38	38	38	38	-38	38	38	38	-38
AQ12	38	38	38	38	38	38	-38	38	38	38	38
AQ13	-32	32	32	32	32	-32	-32	32	-32	-32	32
AQ14	-22	22	-27	22	-27	-15	-4	-18	22	22	-18
AQ15	38	30	38	38	-38	-38	38	-38	38	38	-38
AQ16	-38	-38	-38	-38	-38	-38	-3	-38	-38	-38	-38
AQ17	-25	-25	-25	25	25	-25	-25	-25	25	25	-25
Posts											
AQ18	30	-20	30	-20	30	-10	20	20	-38	30	20
AQ19	30	-20	30	30	-38	20	-10	20	30	-3	20
AQ20	-44	-44	-44	-44	-44	-44	-44	-44	-44	-44	-44
AQ21	-44	-44	-44	-44	-44	-44	-44	-44	-44	-44	44
AQ22	38	38	38	38	38	38	38	38	38	38	-23
AQ23	38	38	38	38	38	38	38	38	38	38	-23
Storage	**Opt 2**	**Opt 2**	**Opt 2**	**Opt 2**	**Opt 2**	**Opt 3**	**Opt 3**	**Opt 1**	**Opt 2**	**Opt 2**	**Opt 1**
AQ24	56	48	56	56	56	10	48	-30	56	56	-30
AQ25	56	49	56	56	56	-30	49	-54	56	56	11
AQ26	49	49	49	49	49	49	49	-20	49	49	20
AQ27	64	64	64	64	64	-39	64	49	64	64	-30
Data collection											
AQ28	32	32	32	32	32	32	32	32	32	32	-32
AQ29	32	32	32	32	32	32	32	32	32	32	-32
Data encryption											
AQ30	69	69	69	69	69	69	69	69	69	69	69
AQ31	44	44	-44	44	44	44	44	-44	44	44	44

D.2 Specific Set

TABLE D.4: Specific score for the reference systems

AQs	Flawed system	Ideal System	AQs	Flawed system	Ideal System
Profile			**Architecture and application**		
AQ1	-35	35	AQ49	-35	35
AQ2	-29	29	AQ50	-29	29
AQ3	-23	23	AQ51	-38	38
AQ4	-23	23	AQ52	-29	29
AQ5	-18	18	AQ53	-18	18
Posts			AQ54	-29	29
AQ6	-13	8	**Settings**		
AQ7	-13	0	AQ55	-27	27
Groups			AQ56	-13	13
AQ8	-38	38	AQ57	-15	15
AQ9	-38	30	**Privacy policies**		
AQ10	-54	54	AQ58	-22	22
AQ11	-43	43	AQ59	-32	32
AQ12	-43	43	AQ60	-22	22
AQ13	-38	38	AQ61	-32	32
AQ14	-27	27	**Feedbacks**		
AQ15	-27	27	AQ62	-20	20
AQ16	-32	54	AQ63	-30	30
Data collection			AQ64	-30	30
AQ17	-32	0	**API and third-party relationships**		
AQ18	-32	0	AQ65	-41	41
AQ19	-32	0	AQ66	-32	32
AQ20	-32	0	AQ67	-75	75
AQ21	-35	0	AQ68	-47	47
AQ22	-40	0			
AQ23	-35	0			
AQ24	-24	0			
Data encryption					
AQ25	0	69			
AQ26	0	64			
AQ27	0	70			
AQ28	0	70			
AQ29	0	44			
AQ30	0	44			
Functionalities					
AQ31	-20	20			
AQ32	-22	22			
AQ33	-20	20			
AQ34	-22	22			
AQ35	-20	20			
AQ36	-20	20			
AQ37	-20	20			
AQ38	-20	20			
AQ39	-22	22			
AQ40	-12	20			
AQ41	-25	0			
AQ42	-22	22			
AQ43	-24	24			
AQ44	-24	24			
AQ45	-24	24			
AQ46	-16	27			
AQ47	-13	22			
AQ48	-13	22			

TABLE D.5: Specific score for the deployed systems

AQs	Facebook	Twitter	Tumblr	Plurk	Pump.io	Diaspora	Twister	Gab	GNU
Profile									
AQ1	35	35	35	35	35	35	-35	35	35
AQ2	29	29	29	29	29	29	-29	29	29
AQ3	-23	-23	23	-23	-23	-23	-23	-23	-23
AQ4	23	23	23	-23	-23	-23	-23	-23	-23
AQ5	18	18	-18	18	-18	-18	-18	-18	-18
Posts									
AQ6	8	-23	8	-23	-23	8	38	23	-38
AQ7	0	38	0	-38	38	0	0	0	38
Groups									
AQ8	-38	-38	0	0	0	0	0	-38	-38
AQ9	10	30	0	0	0	0	0	-38	30
AQ10	-54	-54	0	0	0	0	0	54	54
AQ11	-43	-43	0	0	0	0	0	-43	43
AQ12	-43	-43	0	0	0	0	0	43	43
AQ13	-38	-38	0	0	0	0	0	-38	-38
AQ14	8	-27	0	0	0	0	0	-27	0
AQ15	27	27	0	0	0	0	0	27	27
AQ16	-32	-32	0	0	0	0	0	-32	54
Data collection									
AQ17	32	32	32	32	0	32	0	32	32
AQ18	32	32	32	-32	0	32	0	32	32
AQ19	-32	-32	32	-32	0	-32	0	-32	-32
AQ20	-32	-32	-32	-32	0	-32	0	-32	-32
AQ21	-35	35	-35	-35	0	0	0	-35	35
AQ22	40	40	40	40	0	0	0	40	-40
AQ23	35	-35	-35	-35	0	0	0	-35	-35

AQs	Facebook	Twitter	Tumblr	Plurk	Pump.io	Diaspora	Twister	Gab	GNU
AQ24	-24	-24	-24	-24	0	0	0	-24	-24
Data encryption									
AQ25	0	0	0	0	0	0	69	0	0
AQ26	0	0	0	0	0	0	64	0	0
AQ27	0	0	0	0	0	0	70	0	0
AQ28	0	0	0	0	0	0	70	0	0
AQ29	44	44	44	44	44	44	44	44	44
AQ30	44	44	44	44	44	44	44	44	44
Functionalities									
AQ31	-20	-8	-20	-20	20	11	20	20	-20
AQ32	22	18	18	-3	0	12	0	0	-22
AQ33	-20	-16	-20	-14	20	11	-11	-20	-20
AQ34	22	-22	18	-3	0	12	-22	-22	-22
AQ35	-20	-8	-20	-14	-8	-6	20	-20	-6
AQ36	-20	-20	-20	14	-16	11	20	-20	-20
AQ37	-20	-20	-20	-14	-16	-6	-20	-20	-20
AQ38	-20	-20	-20	-14	0	0	11	-20	11
AQ39	6	18	18	12	0	0	18	-22	0
AQ40	-12	-12	-12	20	20	4	20	20	4
AQ41	-25	25	25	0	0	0	0	0	0
AQ42	-22	-22	-22	-22	-22	-22	22	-22	-22
AQ43	24	24	-24	-24	-24	24	0	-24	-24
AQ44	24	24	-24	-24	-24	24	0	-24	-24
AQ45	-24	-24	-24	-24	24	-24	24	-24	-24
AQ46	-16	-16	27	-16	27	27	27	27	27
AQ47	-13	-13	-13	-13	22	22	22	-13	22
AQ48	-13	-13	-13	22	22	22	22	22	22

AQs	Facebook	Twitter	Tumblr	Plurk	Pump.io	Diaspora	Twister	Gab	GNU
Architecture and application									
AQ49	35	35	35	35	35	35	35	35	35
AQ50	29	29	29	0	0	29	-29	29	0
AQ51	38	38	38	0	0	38	-38	38	0
AQ52	29	29	29	29	0	29	29	29	0
AQ53	18	18	18	18	18	18	-18	18	18
AQ54	29	29	29	0	29	29	-29	29	0
Settings									
AQ55	27	27	27	27	-27	27	27	-27	-27
AQ56	13	13	13	13	13	13	13	13	13
AQ57	-15	-15	-15	-15	-15	-15	-15	-15	0
Privacy policies									
AQ58	22	22	22	22	22	22	-22	22	22
AQ59	-32	32	32	-32	-32	-32	0	-32	-32
AQ60	-22	22	-22	-22	22	22	0	-22	22
AQ61	32	32	32	32	-32	-32	0	32	-32
Feedbacks									
AQ62	-20	20	-20	-20	-20	-20	-20	-20	-20
AQ63	30	30	30	30	-30	30	-30	30	-30
AQ64	30	30	30	30	-30	30	-30	30	-30
API and third-party relationships									
AQ65	41	41	41	41	41	41	41	41	41
AQ66	-32	-32	-32	32	-32	-32	-32	-32	-32
AQ67	-75	-75	75	-75	75	75	75	-75	75
AQ68	-47	-47	-47	-47	-47	47	-47	-47	-47

TABLE D.6: Specific score for the non deployed systems

AQs	PeerSon	Safebook	FETHR	Megaphone	LifeSocial	Cuckoo	Garlanet	HummingBird	DECENT	Cachet	Twitterize
Profile											
AQ1	0	0	0	0	0	0	0	0	0	0	35
AQ2	0	0	0	0	0	0	0	0	0	0	29
AQ3	0	0	0	0	0	0	0	0	0	0	-23
AQ4	0	0	0	0	0	0	0	0	0	0	23
AQ5	0	0	0	0	0	0	0	0	0	0	18
Posts											
AQ6	38	38	0	38	38	38	38	38	38	38	-23
AQ7	0	0	0	0	0	0	0	0	0	0	38
Groups											
AQ8	0	0	0	0	-38	0	0	0	0	0	-38
AQ9	0	0	0	0	0	0	0	0	0	0	30
AQ10	0	0	0	0	0	0	0	0	0	0	-54
AQ11	0	0	0	0	0	0	0	0	0	0	-43
AQ12	0	0	0	0	0	0	0	0	0	0	-43
AQ13	0	0	0	0	0	0	0	0	0	0	-38
AQ14	0	0	0	0	0	0	0	0	0	0	-27
AQ15	0	0	0	0	0	0	0	0	0	0	27
AQ16	0	0	0	0	54	0	0	0	0	0	-32
Data collection											
AQ17	0	0	0	0	0	0	0	0	0	0	32
AQ18	0	0	0	0	0	0	0	0	0	0	32
AQ19	0	0	0	0	0	0	0	0	0	0	-32
AQ20	0	0	0	0	0	0	0	0	0	0	-32
AQ21	0	0	0	0	0	0	0	0	0	0	35
AQ22	0	0	0	0	0	0	0	0	0	0	40
AQ23	0	0	0	0	0	0	0	0	0	0	-35

AQs	PeerSon	Safebook	FETHR	Megaphone	LifeSocial	Cuckoo	Garlanet	HummingBird	DECENT	Cachet	Twitterize
AQ24	0	0	0	0	0	0	0	0	0	0	-24
Data encryption											
AQ25	0	0	0	69	0	0	69	69	69	69	69
AQ26	0	0	0	64	0	0	64	64	64	64	64
AQ27	0	-28	0	70	70	-28	70	-42	70	70	70
AQ28	0	70	0	70	70	-28	70	-42	70	70	-42
AQ29	0	0	0	44	0	0	0	44	44	44	44
AQ30	0	0	0	44	0	0	0	44	44	44	44
Functionalities											
AQ31	0	11	0	20	0	0	20	0	20	20	-8
AQ32	0	18	0	12	0	0	0	0	12	12	18
AQ33	0	0	0	0	0	0	0	0	20	20	-16
AQ34	0	0	0	0	0	0	0	0	12	12	-22
AQ35	0	0	0	11	0	-3	0	0	0	0	-8
AQ36	0	0	0	11	0	-20	0	0	0	0	-20
AQ37	-3	0	0	11	0	20	0	0	11	11	-20
AQ38	20	-6	0	20	-20	-20	0	0	0	0	-20
AQ39	12	0	0	12	-22	0	0	0	0	0	18
AQ40	20	20	0	20	20	20	20	12	20	20	-12
AQ41	0	0	0	0	0	0	0	0	0	0	25
AQ42	-22	-22	-22	22	0	-22	22	0	-22	-22	-22
AQ43	-24	0	-24	0	0	24	0	0	24	24	24
AQ44	-24	0	0	0	0	24	0	0	0	0	24
AQ45	0	0	24	24	0	0	24	24	0	0	-24
AQ46	27	27	27	27	27	27	27	27	27	27	-16
AQ47	22	22	22	22	22	22	22	22	22	22	-13
AQ48	22	22	22	22	22	22	22	22	22	22	-13

AQs	PeerSon	Safebook	FETHR	Megaphone	LifeSocial	Cuckoo	Garlanet	HummingBird	DECENT	Cachet	Twitterize
Architecture and application											
AQ49	0	0	0	0	0	0	35	0	0	0	0
AQ50	0	0	0	0	0	0	0	0	0	0	0
AQ51	0	0	0	0	0	0	0	0	0	0	0
AQ52	0	0	0	0	0	0	29	0	0	0	0
AQ53	0	0	0	0	0	0	18	0	0	0	0
AQ54	0	0	0	0	0	0	0	0	0	0	0
Settings											
AQ55	0	0	0	0	0	0	-27	0	0	0	27
AQ56	0	0	0	0	0	0	13	0	0	0	13
AQ57	0	0	0	0	0	0	0	0	0	0	-15
Privacy policies											
AQ58	0	0	0	0	0	0	-22	0	0	0	0
AQ59	0	0	0	0	0	0	0	0	0	0	0
AQ60	0	0	0	0	0	0	0	0	0	0	0
AQ61	0	0	0	0	0	0	0	0	0	0	0
Feedbacks											
AQ62	0	0	0	0	0	0	0	0	0	0	20
AQ63	0	0	0	0	0	0	0	0	0	0	30
AQ64	0	0	0	0	0	0	0	0	0	0	30
API and third-party relationships											
AQ65	0	0	0	0	0	0	41	41	0	0	41
AQ66	0	0	0	0	0	0	32	0	0	0	0
AQ67	0	0	0	0	0	0	75	0	0	0	0
AQ68	0	0	0	0	0	0	0	0	0	0	0

Bibliography

[1] Albert-László Barabási. *Linked: The new science of networks*. 2003. URL: http://www.mta.t-mobile.mpt.bme.hu/dok/8_Barabasi.pdf.

[2] Laura Garton, Caraline Haythornthwaite, and Barry Wellman. "Studying online social networks". In: *Journal of Computer-Mediated Communication* 3.1 (2004). DOI: 10.1111/j.1083-6101.1997.tb00062.x.

[3] Sixdegrees. *Six Degrees Social Engine*. 1997. URL: http://sixdegrees.com/.

[4] Alexander Richter and Michael Koch. "Functions of social networking services". In: *From CSCW to Web 2.0: European Developments in Collaborative Design Selected Papers from COOP08* (2008).

[5] Danah M Boyd and Nicole B Ellison. "Social network sites: Definition, history, and scholarship". In: *Journal of computer-mediated Communication* 13.1 (2007), pp. 210–230.

[6] Andreas M. Kaplan and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media". In: *Business horizons* 53.1 (2010), pp. 59–68. DOI: 10.1016/j.bushor.2009.09.003.

[7] Statista. *Number of social media users worldwide from 2010 to 2021 (in billions)*. 2019. URL: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[8] W. Glynn Mangold and David J. Faulds. "Social media: The new hybrid element of the promotion mix". In: *Business Horizons* 52.4 (2009), pp. 357–365. DOI: 10.1016/j.bushor.2009.03.002.

[9] Habibul Haque Khondker. "Role of the New Media in the Arab Spring". In: *Globalizations* 8.5 (2011), 675—679. DOI: 10.1080/14747731.2011.621287.

[10] Panagiotis Panagiotopoulos, Alinaghi Ziaee Bigdeli, and Steven Sams. "Citizen–government collaboration on social media: The case of Twitter in the 2011 riots in England". In: *Government Information Quarterly* 31.3 (2014), 349––357. DOI: 10.1016/j.giq.2013.10.014.

[11] Theguardian. *Facebook, Instagram and WhatsApp suffer outages in Americas and Europe*. 2019. URL: https://www.theguardian.com/technology/2019/mar/13/facebook-outages-americas-europe-instagram-whatsapp.

[12] pleaserobme.com. *Raising awareness about over-sharing*. 2019. URL: http://pleaserobme.com/.

[13] Pia Gadkari. *How does Twitter make money?* Nov. 2013. URL: http://www.bbc.com/news/business-24397472.w.

[14] Benjamin C. M. Fung, Ke Wang, and Philip S. Yu. "Anonymizing Classification Data for Privacy Preservation". In: *IEEE Trans. on Knowl. and Data Eng.* 19.5 (May 2007), pp. 711–725. ISSN: 1041-4347. DOI: 10.1109/TKDE.2007.1015. URL: http://dx.doi.org/10.1109/TKDE.2007.1015.

[15] Yves-Alexandre de Montjoye et al. "Unique in the Crowd: The privacy bounds of human mobility". In: 3.1376 (Mar. 2013). DOI: 10.1038/srep01376. URL: http://dx.doi.org/10.1038/srep01376.

[16] Yves-Alexandre de Montjoye et al. "Unique in the shopping mall: On the reidentifiability of credit card metadata". In: *Science* 347.6221 (2015), pp. 536–539. ISSN: 0036-8075. DOI: 10.1126/science.1256297. URL: http://science.sciencemag.org/content/347/6221/536.

[17] Jan Philipp Albrecht. *Legislative train schedule | European Parliament*. 2016. URL: http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-general-data-protection-regulation.

[18] EUGDPR. *The EU General Data Protection Regulation*. 2018. URL: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[19] Dara Hallinan, Michael Friedewald, and Paul Mccarthy. "Citizens Perceptions of Data Protection and Privacy in Europe". In: *Computer Law & Security Review* 28.3 (June 2012), pp. 263–272. ISSN: 02673649. DOI: 10.1016/j.clsr.2012.03.005. URL: https://linkinghub.elsevier.com/retrieve/pii/S026736491200057X.

[20] Tiffany Robertson. *Top five concerns with GDPR compliance*. Apr. 2018. URL: https://blogs.thomsonreuters.com/financial-risk/risk-management-and-compliance/top-five-concerns-gdpr-compliance/.

[21] Patrick Greenfield. *The Cambridge Analytica Files: The Story so Far*. 2018. URL: https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

[22] Emma Graham-Harrison and Carole Cadwalladr. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Mar. 2018. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[23] Statista. *Facebook users worldwide 2019*. 2019. URL: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[24] Isabell Büschel et al. "Protecting Human Health and Security in Digital Europe: How to Deal with the "Privacy Paradox"?" In: *Science and Engineering Ethics* 20.3 (Sept. 2014), pp. 639–658. ISSN: 1471-5546. DOI: 10.1007/s11948-013-9511-y.

[25] Dara Hallinan, Michael Friedewald, and Paul McCarthy. "Citizens' perceptions of data protection and privacy in Europe". In: *Computer Law & Security Review* 28.3 (June 2012), pp. 263–272. ISSN: 0267-3649. DOI: http://dx.doi.org/10.1016/j.clsr.2012.03.005. URL: http://www.sciencedirect.com/science/article/pii/S026736491200057X.

[26] James Q. Whitman. "The Two Western Cultures of Privacy: Dignity versus Liberty". In: *The Yale Law Journal* 113.6 (Apr. 2004), p. 1151. ISSN: 00440094. DOI: 10.2307/4135723. URL: https://www.jstor.org/stable/10.2307/4135723?origin=crossref.

[27] Akshay Java et al. "Why We Twitter: Understanding Microblogging Usage and Communities". In: *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining and Social Network Analysis*. WebKDD/SNA-KDD '07. San Jose, California: ACM, 2007, pp. 56–65. ISBN: 978-1-59593-848-0. DOI: 10.1145/1348549.1348556. URL: http://doi.acm.org/10.1145/1348549.1348556.

[28] Twitter. 2019. URL: https://twitter.com/.

[29] Statista. *Number of monthly active Twitter users worldwide from 1st quarter 2010 to 1st quarter 2019 (in millions)*. 2019. URL: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

[30] Briony J Oates. *Researching information systems and computing*. Sage, 2006.

[31] Haewoon Kwak et al. "What is Twitter, a Social Network or a News Media?" In: *Proceedings of the 19th International Conference on World Wide Web*. WWW '10. Raleigh, North Carolina, USA: ACM, 2010, pp. 591–600. ISBN: 978-1-60558-799-8. DOI: 10.1145/1772690.1772751. URL: http://doi.acm.org/10.1145/1772690.1772751.

[32] Thomas Aichner and Frank Jacob. "Measuring the degree of corporate social media use". In: *International Journal of Market Research* 57.2 (2015), pp. 257–275. DOI: 10.2501/IJMR-2015-018. URL: https://doi.org/10.2501/IJMR-2015-018.

[33] Prachi Kumari. "Requirements analysis for privacy in social networks". In: *8th Intl. Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods (VG)*. 2010.

[34] Johannes Buchmann. *Internet Privacy: Options for adequate realisation*. Springer Science & Business Media, 2013. ISBN: 978-3-642-37913-0. DOI: 10.1007/978-3-642-37913-0.

[35] Bruce Schneier. "A Taxonomy of Social Networking Data". In: *IEEE Security and Privacy* 8 (2010), p. 88. ISSN: 1540-7993. DOI: doi.ieeecomputersociety.org/10.1109/MSP.2010.118.

[36] UN. *Universal Declaration of Human Rights*. 2016. URL: http://www.un.org/en/universal-declaration-human-rights.

[37] Oxforddictionarie. *Privacy | Definition of Privacy in English by Oxford Dictionaries*. 2019. URL: https://en.oxforddictionaries.com/definition/privacy.

[38] Sameer Patil and Alfred Kobsa. "Privacy Considerations in Awareness Systems: Designing with Privacy in Mind". In: *Awareness Systems: Advances in Theory, Methodology and Design*. Springer, 2009, pp. 187–206.

[39] LII Staff. *Privacy*. Sept. 2017. URL: https://www.law.cornell.edu/wex/privacy.

[40] Qun Ni et al. "Privacy-aware role-based access control". In: *ACM Transactions on Information and System Security (TISSEC)* 13.3 (2010), p. 24.

[41] James Rachels. "Why Privacy is Important". In: *Philosophy & Public Affairs* 4.4 (1975), pp. 323–333. ISSN: 00483915, 10884963.

[42] Alan F Westin. *Privacy and freedom*. Vol. 1. New York, USA: Atheneum, 1967.

[43] Alan F Westin. "Social and political dimensions of privacy". In: *Journal of social issues* 59.2 (2003), pp. 431–453.

[44] Christian Bunnig and Clemens H Cap. "Ad Hoc Privacy Management in Ubiquitous Computing Environments". In: *Second International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2009. CENTRIC'09*. IEEE, Sept. 2009, pp. 85–90. ISBN: 978-1-4244-4781-7. DOI: 10.1109/CENTRIC.2009.20. URL: http://ieeexplore.ieee.org/document/5291015/.

[45] Somayeh Taheri, Salke Hartung, and Dieter Hogrefe. "Achieving Receiver Location Privacy in Mobile Ad Hoc Networks". In: *2010 IEEE Second International Conference on Social Computing*. IEEE, Aug. 2010, pp. 800–807. ISBN: 978-1-4244-8439-3. DOI: 10.1109/SocialCom.2010.122. URL: http://ieeexplore.ieee.org/document/5591466/.

[46] Stefan Weiss. "The need for a paradigm shift in addressing privacy risks in social networking applications". In: *The future of identity in the information society*. Boston, USA: Springer, June 2008, pp. 161–171. DOI: 10.1007/978-0-387-79026-8_12.

[47] OECD. *OECDprivacy.org*. 2019. URL: http://oecdprivacy.org/.

[48] OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 2013. URL: https://bit.ly/1gaZQzY.

[49] MThree. *The Six Privacy Principles of GDPR*. 2017. URL: https://www.mthreeconsulting.com/blog/2017/04/the-6-privacy-principles-of-gdpr.

[50] consultancy.uk. *Six privacy principles for General Data Protection Regulation compliance*. 2017. URL: https://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance.

[51] PIPEDA. *The 10 Privacy Principles of PIPEDA*. Aug. 2015. URL: http://www.privacysense.net/10-privacy-principles-of-pipeda/.

[52] ISACA. *Trust In, and Value From, Information Systems*. 2019. URL: https://www.isaca.org/pages/default.aspx.

[53] ISACA. *ISACA Privacy Principles and Program Management Guide*. 2019. URL: https://bit.ly/2zuXwBL.

[54] ISO. *ISO - International Organization for Standardization*. June 2017. URL: https://www.iso.org/standard/45123.html.

[55] ISO. *Information technology – Security techniques – Privacy framework*. 1st ed. 2019, 1—21. URL: https://bit.ly/2GvnnOt.

[56] Federal Information Processing et al. *Standards for Security Categorization of Federal Information and Information Systems*. 2004. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[57] S. Harris. *CISSP all-in-one exam guide*. McGraw-Hill, 2012.

[58] Marit Hansen, Meiko Jensen, and Martin Rost. "Protection Goals for Privacy Engineering". In: *2015 IEEE Security and Privacy Workshops*. IEEE, May 2015, pp. 159–166. DOI: 10.1109/SPW.2015.13.

[59] Matt Bishop. *Introduction to computer security, 1st ed*. 1st edition. Boston: Addison-Wesley, 2008.

[60] Michael Hafner and Ruth Breu. "Basic concepts of soa security". In: *Security Engineering for Service-Oriented Architectures* (2009), pp. 27–45.

[61] distrinet.cs.kuleuven.be. *LINDDUN privacy threat modeling*. 2019. URL: https://distrinet.cs.kuleuven.be/software/linddun/.

[62] Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. "Addressing privacy requirements in system design: the PriS method". In: *Requirements Engineering* 13.3 (Sept. 2008), pp. 241–255. ISSN: 1432-010X. DOI: 10.1007/s00766-008-0067-3. URL: https://doi.org/10.1007/s00766-008-0067-3.

[63] Andreas Pfitzmann and Marit Hansen. *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. 2010. URL: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[64] Michael John Rogers. "Private and Censorship-Resistant Communication over Public Networks". PhD thesis. University College London University of London: Department of Computer Science, 2010.

[65] Martin Rost and Andreas Pfitzmann. "Datenschutz-Schutzziele — revisited". In: *Datenschutz und Datensicherheit - DuD* 33.6 (June 2009), pp. 353–358. ISSN: 1862-2607. DOI: 10.1007/s11623-009-0072-9.

[66] Marit Hansen. "Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals". In: *IFIP Advances in Information and Communication Technology Privacy and Identity Management for Life* (2012), 14—31. DOI: 10.1007/978-3-642-31668-5_2.

[67] Martin Rost and Kirsten Bock. *Privacy by Design and the New Protection Goals*. 2011.

[68] nist. *National Institute of Standards and Technology*. 2019. URL: https://www.nist.gov/.

[69] Sean Brooks et al. *Privacy Risk Management for Federal Information Systems*. 2015.

[70] Stefan Weiss. "The Need for a Paradigm Shift in Addressing Privacy Risks in Social Networking Applications". In: *IFIP International Summer School on the Future of Identity in the Information Society*. Springer, 2007, pp. 161–171.

[71] G NaliniPriya and M Asswini. "A survey on vulnerable attacks in online social networks". In: *International Confernce on Innovation Information in Computing Technologies*. IEEE, Feb. 2015, pp. 1–6. DOI: 10.1109/ICIICT.2015.7396102.

[72] Jon Russell. *Prominent Twitter accounts compromised after third-party app Twitter Counter hacked*. Mar. 2017. URL: https://techcrunch.com/2017/03/15/twitter-counter-hacked/.

[73] Michael Beye et al. *Literature overview-privacy in online social networks*. 2010. URL: https://ris.utwente.nl/ws/portalfiles/portal/5095526/literaturereview.pdf.

[74] Carlos Laorden et al. "A Threat Model Approach to Threats and Vulnerabilities in On-line Social Networks". In: *Computational Intelligence in Security for Information Systems 2010*. Berlin, Heidelberg: Springer, 2010, pp. 135–142. ISBN: 978-3-642-16626-6.

[75] Leucio Antonio Cutillo, Mark Manulis, and Thorsten Strufe. *Security and privacy in online social networks*. Boston, MA: Springer US, 2010, pp. 497–522. DOI: 10.1007/978-1-4419-7142-5_16.

[76] Elena Zheleva, Evimaria Terzi, and Lise Getoor. *Privacy in Social Networks*. San Rafael, CA: Morgan & Claypool Publishers, 2012. ISBN: 9781608458639.

[77] Muhammad Al-Qurishi et al. "Sybil Defense Techniques in Online Social Networks: A Survey". In: *IEEE Access* 5 (2017), pp. 1200–1219. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2656635.

[78] Hongyu Gao et al. "Security Issues in Online Social Networks". In: *IEEE Internet Computing* 15 (July 2011), pp. 56–63. ISSN: 1089-7801. DOI: 10.1109/MIC.2011.50.

[79] Leyla Bilge et al. "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. Madrid, Spain: ACM, 2009, pp. 551–560. ISBN: 978-1-60558-487-4. DOI: 10.1145/1526709.1526784. URL: http://doi.acm.org/10.1145/1526709.1526784.

[80] OWASP. *SQL Injection*. Oct. 2016. URL: https://www.owasp.org/index.php/SQL_Injection.

[81] Guanhua Yan et al. "Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications". In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ASIACCS '11. Hong Kong, China: ACM, 2011, pp. 196–206. ISBN: 978-1-4503-0564-8. DOI: 10.1145/1966913.1966939. URL: http://doi.acm.org/10.1145/1966913.1966939.

[82] Pooja Chaudhary, B. B Gupta, and Shashank Gupta. "Cross-site scripting (XSS) worms in Online Social Network (OSN): Taxonomy and defensive mechanisms". In: *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. Mar. 2016, pp. 2131–2136.

[83] Imrul Kayes and Adriana Iamnitchi. "A Survey on Privacy and Security in Online Social Networks". In: *CoRR* abs/1504.03342 (2015). arXiv: 1504.03342. URL: http://arxiv.org/abs/1504.03342.

[84] Tom N. Jagatic et al. "Social Phishing". In: *ACM Communication* 50.10 (Oct. 2007), pp. 94–100. ISSN: 0001-0782. DOI: 10.1145/1290958.1290968. URL: http://doi.acm.org/10.1145/1290958.1290968.

[85] Claudia Canali, Michele Colajanni, and Riccardo Lancellotti. "Data acquisition in social networks: Issues and proposals". In: *Proceedings of the International Workshop on Services and Open Sources (SOS'11)*. 2011.

[86] Jane Henriksen-Bulmer and Sheridan Jeary. "Re-identification attacks - A systematic literature review". In: *International Journal of Information Management* 36.6, Part B (2016), pp. 1184–1192. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2016.08.002. URL: http://www.sciencedirect.com/science/article/pii/S0268401215301262.

[87] Gilbert Wondracek et al. "A Practical Attack to De-anonymize Social Network Users". In: *Proceedings of the 2010 IEEE Symposium on Security and Privacy*. SP '10. IEEE Computer Society, 2010, pp. 223–238. ISBN: 978-0-7695-4035-1. DOI: 10.1109/SP.2010.21. URL: http://dx.doi.org/10.1109/SP.2010.21.

[88] IC3. *Internet Crime Schemes*. 2019. URL: https://bit.ly/2zrr43i.

[89] Ubaid Ur Rehman et al. "On detection and prevention of clickjacking attack for osns". In: *2013 11th International Conference on Frontiers of Information Technology (FIT)*. IEEE, 2013, pp. 160–165.

[90] Michael Fire, Roy Goldschmidt, and yuval Elovici. "Online Social Networks: Threats and Solutions". In: *IEEE Communications Surveys Tutorials* 16.4 (2014), pp. 2019–2036. ISSN: 1553-877X. DOI: 10.1109/COMST.2014.2321628.

[91] Prateek Dewan and Ponnurangam Kumaraguru. "Detecting Malicious Content on Facebook". In: *CoRR* abs/1501.00802 (2015). arXiv: 1501.00802. URL: http://arxiv.org/abs/1501.00802.

[92] GOsafeonline. *Social Engineering on Social Media*. June 2017. URL: https://bit.ly/2LhmhXE.

[93] Deepak Chandrasekaran, David Costello, and Paul Stubbs. *Social media profiling*. US Patent App. 13/465,335. Nov. 2013. URL: https://www.google.com/patents/US20130297619.

[94] Electronic Privacy Information Center. *EPIC - Privacy and Consumer Profiling*. 2019. URL: https://www.epic.org/privacy/profiling/.

[95] Qiang Cao et al. "Aiding the Detection of Fake Accounts in Large Scale Social Online Services". In: *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*. NSDI'12. San Jose, CA: USENIX Association, 2012, pp. 15–15. URL: http://dl.acm.org/citation.cfm?id=2228298.2228319.

[96] Arvind Narayanan and Vitaly Shmatikov. "De-anonymizing social networks". In: *2009 30th IEEE Symposium on Security and Privacy*. Oakland, California: IEEE, 2009, pp. 173–187.

[97] Jianwei Qian et al. "De-anonymizing social networks and inferring private attributes using knowledge graphs". In: *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. San Francisco, USA: IEEE, 2016, pp. 1–9.

[98] Michael Hay et al. "Resisting Structural Re-identification in Anonymized Social Networks". In: *Proc. VLDB Endow.* 1.1 (Aug. 2008), pp. 102–114. ISSN: 2150-8097. DOI: 10.14778/1453856.1453873.

[99] Pierangela Samarati and Latanya Sweeney. *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*. 1998. URL: https://epic.org/privacy/reidentification/Samarati_Sweeney_paper.pdf.

[100] Kun Liu and Evimaria Terzi. "Towards Identity Anonymization on Graphs". In: *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*. SIGMOD '08. Vancouver, Canada: ACM, 2008, pp. 93–106. ISBN: 978-1-60558-102-6. DOI: 10.1145/1376616.1376629.

[101] Cynthia Dwork et al. "Calibrating noise to sensitivity in private data analysis". In: *Theory of cryptography conference*. New York, USA: Springer, 2006, pp. 265–284.

[102] Cynthia Dwork. "Differential privacy: A survey of results". In: *International Conference on Theory and Applications of Models of Computation*. Xi'an, China: Springer, 2008, pp. 1–19.

[103] Rui Chen, Gergely Acs, and Claude Castelluccia. "Differentially Private Sequential Data Publication via Variable-length N-grams". In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS '12. Raleigh, North Carolina, USA: ACM, 2012, pp. 638–649. ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382263.

[104] Imrul Kayes and Adriana Iamnitchi. "Privacy and security in online social networks: A survey". In: *Online Social Networks and Media* 3 (Oct. 2017), pp. 1–21. DOI: 10.1016/j.osnem.2017.09.001.

[105] Anwitaman Datta et al. "Decentralized Online Social Networks". In: *Handbook of Social Network Technologies and Applications*. Boston, MA: Springer US, 2010, pp. 349–378. ISBN: 978-1-4419-7142-5. DOI: 10.1007/978-1-4419-7142-5_17.

[106] Sonia Jahid, Prateek Mittal, and Nikita Borisov. "EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation". In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ASIACCS '11. Hong Kong, China: ACM, 2011, pp. 411–415. ISBN: 978-1-4503-0564-8. DOI: 10.1145/1966913.1966970.

[107] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption". In: *2007 IEEE Symposium on Security and Privacy (SP '07)*. Oakland, California, USA: IEEE, May 2007, pp. 321–334. DOI: 10.1109/SP.2007.11.

[108] Facebook. *What is two-factor authentication and how does it work?* 2018. URL: https://www.facebook.com/help/148233965247823.

[109] Twitter. *How to use login verification*. 2018. URL: https://help.twitter.com/en/managing-your-account/two-factor-authentication.

[110] Sangho Lee and Jong Kim. "WarningBird: Detecting Suspicious URLs in Twitter Stream". In: *IEEE Transactions on Dependable and Secure Computing* 10.3 (June 2013), pp. 183–195. ISSN: 1545-5971. DOI: 10.1109/TDSC.2013.3.

[111] Anupama Aggarwal, Ashwin Rajadesingan, and Ponnurangam Kumaraguru. "PhishAri: Automatic realtime phishing detection on twitter". In: *2012 eCrime Researchers Summit*. Las Croabas, PR, USA: IEEE, Oct. 2012, pp. 1–12.

[112] Sajid Yousuf Bhat and Muhammad Abulaish. "Community-based features for identifying spammers in online social networks". In: *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. Niagara Falls, Canada: IEEE, Aug. 2013, pp. 100–107.

[113] Enkh-Amgalan Baatarjav, Ram Dantu, and Santi Phithakkitnukoon. "Privacy management for facebook". In: *International Conference on Information Systems Security*. Hyderabad, India: Springer, 2008, pp. 273–286.

[114] Lujun Fang and Kristen LeFevre. "Privacy wizards for social networking sites". In: *Proceedings of the 19th international conference on World wide web*. North Carolina, USA: ACM, 2010, pp. 351–360.

[115] Igor Bilogrevic et al. "A machine-learning based approach to privacy-aware information-sharing in mobile social networks". In: *Pervasive and Mobile Computing* 25 (Jan. 2016), pp. 125–142. DOI: 10.1016/j.pmcj.2015.01.006.

[116] Yuan Cheng, Jaehong Park, and Ravi Sandhu. "An access control model for online social networks using user-to-user relationships". In: *IEEE transactions on dependable and secure computing* 13.4 (July 2016), pp. 424–436. DOI: 10.1109/TDSC.2015.2406705.

[117] Oxforddictionarie. *Metric | Definition of Metric in English by Oxford Dictionaries*. 2019. URL: https://en.oxforddictionaries.com/definition/metric.

[118] NIST and Emmanuel Aroms. *NIST Special Publication 800-55 Rev1 Security Metrics Guide for Information Technology Systems*. Paramount, CA: NIST, 2012. ISBN: 1470152045, 9781470152048.

[119] Shirley C Payne. *SANS: A Guide to Security Metrics*. June 2006. URL: https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55.

[120] Ms Deepti Juneja, Ms Kavita Arora, and Ms Sonia Duggal. "Developing security metrics for information security measurement system". In: *International Journal of Enterprise Computing and Business Systems* 1.2 (2011).

[121] Rana Khudhair Abbas Ahmed. "Overview of Security Metrics, Software Engineering". In: *Electrical & Computer Science* 4.4 (2016), pp. 59–64. DOI: 10.11648/j.se.20160404.11.

[122] Elizabeth Chew et al. *Performance measurement guide for information security*. Tech. rep. 800-55 Rev 1. 2008.

[123] David A Chapin and Steven Akridge. "How can security be measured". In: *information systems control journal* 2.1 (2005).

[124] Andrew Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education, 2007.

[125] *ISO/IEC 27004:2016*. Dec. 2016. URL: https://www.iso.org/standard/64120.html.

[126] Robert Hachett. "LinkedIn Lost 167 Million Account Credentials in Data Breach". In: *Fortune* (2016). URL: http://fortune.com/2016/05/18/linkedin-data-breach-email-password/.

[127] Michael K. Reiter and Aviel D. Rubin. "Crowds: Anonymity for Web Transactions". In: *ACM Trans. Inf. Syst. Secur.* 1.1 (Nov. 1998), pp. 66–92. ISSN: 1094-9224. DOI: 10.1145/290163.290168. URL: http://doi.acm.org/10.1145/290163.290168.

[128] Oliver Berthold, Andreas Pfitzmann, and Ronny Standtke. "The Disadvantages of Free MIX Routes and How to Overcome Them". In: *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*. Springer, 2001, pp. 30–45. ISBN: 3-540-41724-9. URL: http://dl.acm.org/citation.cfm?id=371931.371975.

[129] Andrei Serjantov and George Danezis. "Towards an Information Theoretic Metric for Anonymity". In: *Privacy Enhancing Technologies: Second International Workshop*. San Francisco, CA, USA: Springer Berlin Heidelberg, Apr. 2003, pp. 41–53. ISBN: 978-3-540-36467-2. DOI: 10.1007/3-540-36467-6_4. URL: https://doi.org/10.1007/3-540-36467-6_4.

[130] Claudia Díaz et al. "Towards Measuring Anonymity". In: *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*. PET'02. San Francisco, CA, USA: Springer-Verlag, 2003, pp. 54–68. ISBN: 3-540-00565-X.

[131] Claudia Diaz. "Anonymity Metrics Revisited". In: *Anonymous Communication and its Applications*. Dagstuhl Seminar Proceedings 05411. Dagstuhl, Germany: Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, 2006. URL: http://drops.dagstuhl.de/opus/volltexte/2006/483.

[132] Gergely Tóth, Zoltán Hornák, and Ferenc Vajda. "Measuring anonymity revisited". In: In Proceedings of the Ninth Nordic Workshop on Secure IT Systems, 2004, pp. 85–90.

[133] Sebastian Clauß and Stefan Schiffner. "Structuring Anonymity Metrics". In: *Proceedings of the Second ACM Workshop on Digital Identity Management*. DIM '06. Alexandria, Virginia, USA: ACM, 2006, pp. 55–62. ISBN: 1-59593-547-9. DOI: 10.1145/1179529.1179539. URL: http://doi.acm.org/10.1145/1179529.1179539.

[134] Christer Andersson and Reine Lundin. "On the Fundamentals of Anonymity Metrics". In: *The Future of Identity in the Information Society: Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society*. Karlstad University, Sweden, Springer US, Aug. 2008, pp. 325–341. ISBN: 978-0-387-79026-8. DOI: 10.1007/978-0-387-79026-8_23. URL: https://doi.org/10.1007/978-0-387-79026-8_23.

[135] S. Mauw, J. H. S. Verschuren, and E. P. de Vink. "A Formalization of Anonymity and Onion Routing". In: *Computer Security – ESORICS 2004: 9th European Symposium on Research in Computer Security*. Sophia Antipolis, France: Springer Berlin Heidelberg, Sept. 2004, pp. 109–124. ISBN: 978-3-540-30108-0. DOI: 10.1007/978-3-540-30108-0_7. URL: https://doi.org/10.1007/978-3-540-30108-0_7.

[136] Joan Feigenbaum, Aaron Johnson, and Paul Syverson. "A Model of Onion Routing with Provable Anonymity". In: *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security*. Scarborough, Trinidad and Tobago: Springer Berlin Heidelberg, Feb. 2007, pp. 57–71. ISBN: 978-3-540-77366-5. DOI: 10.1007/978-3-540-77366-5_9. URL: https://doi.org/10.1007/978-3-540-77366-5_9.

[137] Aaron Beach, Mike Gartrell, and Richard Han. "q-Anon: Rethinking Anonymity for Social Networks". In: *Proceedings of the 2010 IEEE Second International Conference on Social Computing*. SOCIALCOM '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 185–192. ISBN: 978-0-7695-4211-9. DOI: 10.1109/SocialCom.2010.34. URL: http://dx.doi.org/10.1109/SocialCom.2010.34.

[138] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity". In: *2007 IEEE 23rd International Conference on Data Engineering*. IEEE Computer Society, Apr. 2007, pp. 106–115. DOI: 10.1109/ICDE.2007.367856.

[139] Komei Kamiyama et al. "Unified Metric for Measuring Anonymity and Privacy with Application to Online Social Network". In: *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Oct. 2010, pp. 506–509. DOI: 10.1109/IIHMSP.2010.129.

[140] Silvia Puglisi, David Rebollo-Monedero, and Jordi Forné. "On the Anonymity Risk of Time-Varying User Profiles". In: *Entropy* 19.5 (2017), p. 190.

[141] Javier Parra-Arnau, David Rebollo-Monedero, and Jordi Forné. "Measuring the privacy of user profiles in personalized information systems". In: *Future Generation Computer Systems* 33 (2014), pp. 53–63.

[142] Michael E. Maximilien et al. "Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform". In: *Proceedings of W2SP 2009: Web 2.0 Security and Privacy*. Oakland, CA, USA, May 2009. URL: http://w2spconf.com/2009/papers/s4p2.pdf.

[143] Kun Liu and Evimaria Terzi. "A Framework for Computing the Privacy Scores of Users in Online Social Networks". In: *ACM Trans. Knowl. Discov. Data* 5.1 (Dec. 2010), 6:1–6:30. ISSN: 1556-4681. DOI: 10.1145/1870096.1870102. URL: http://doi.acm.org/10.1145/1870096.1870102.

[144] Agrima Srivastava and G Geethakumari. "Measuring privacy leaks in Online Social Networks". In: *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. Aug. 2013, pp. 2095–2100. DOI: 10.1109/ICACCI.2013.6637504.

[145] Georgios Petkos, Symeon Papadopoulos, and Yiannis Kompatsiaris. "PScore: A Framework for Enhancing Privacy Awareness in Online Social Networks". In: *2015 10th International Conference on Availability, Reliability and Security*. Aug. 2015, pp. 592–600. DOI: 10.1109/ARES.2015.80.

[146] Ruggero G. Pensa and Gianpiero Di Blasi. "A privacy self-assessment framework for online social networks". In: *Expert Systems with Applications* 86 (2017), pp. 18 –31. ISSN: 0957-4174. DOI: http://dx.doi.org/10.1016/j.eswa.2017.05.054. URL: http://www.sciencedirect.com/science/article/pii/S0957417417303767.

[147] Joseph Bonneau and Sören Preibusch. "The Privacy Jungle:On the Market for Data Protection in Social Networks". In: *Economics of Information Security and Privacy*. Boston, MA: Springer US, 2010, pp. 121–167. ISBN: 978-1-4419-6967-5. DOI: 10.1007/978-1-4419-6967-5_8. URL: https://doi.org/10.1007/978-1-4419-6967-5_8.

[148] Justin Becker and Hao Chen. "Measuring Privacy Risk in Online Social Networks". In: University of California, Davis, 2009.

[149] Tran Hong Ngoc et al. "New Approach to Quantification of Privacy on Social Network Sites". In: *Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications*. AINA '10. IEEE Computer Society, 2010, pp. 556–564. ISBN: 978-0-7695-4018-4. DOI: 10.1109/AINA.2010.118. URL: http://dx.doi.org/10.1109/AINA.2010.118.

[150] Nilothpal Talukder et al. "Privometer: Privacy protection in social networks". In: *2010 IEEE 26th International Conference on Data Engineering Workshops (ICDEW 2010)*. IEEE Computer Society, Mar. 2010, pp. 266–269. DOI: 10.1109/ICDEW.2010.5452715.

[151] Cuneyt Akcora, Barbara Carminati, and Elena Ferrari. "Privacy in Social Networks: How Risky is Your Social Graph?" In: *2012 IEEE 28th International Conference on Data Engineering*. IEEE Computer Society, Apr. 2012, pp. 9–19. DOI: 10.1109/ICDE.2012.99.

[152] BS Vidyalakshmi, Raymond K Wong, and Chi-Hung Chi. "Privacy scoring of social network users as a service". In: *2015 IEEE International Conference on Services Computing (SCC)*. IEEE, 2015, pp. 218–225.

[153] Raj Kumar Nepali and Yong Wang. "SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking". In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*. IEEE Computer Society, July 2013, pp. 162–166. DOI: 10.1109/ICDCSW.2013.49.

[154] Yong Wang and Raj Kumar Nepali. "Privacy Measurement for Social Network Actor Model". In: *2013 International Conference on Social Computing*. Sept. 2013, pp. 659–664. DOI: 10.1109/SocialCom.2013.99.

[155] Yong Wang, Raj Kumar Nepali, and Jason Nikolai. "Social network privacy measurement and simulation". In: *2014 International Conference on Computing, Networking and Communications (ICNC)*. Feb. 2014, pp. 802–806. DOI: 10.1109/ICCNC.2014.6785440.

[156] Isabell Büschel et al. "Protecting Human Health and Security In Digital Europe: How to Deal with the "Privacy Paradox"?" In: *Science and Engineering Ethics* 20.3 (Sept. 2014), pp. 639–658. ISSN: 1353-3452. DOI: 10.1007/s11948-013-9511-y. URL: http://link.springer.com/10.1007/s11948-013-9511-y.

[157] Ardion .D Beldad and Sabrina .M Hegner. "More Photos From Me to Thee: Factors Influencing the Intention to Continue Sharing Personal Photos on an Online Social Networking (OSN) Site Among Young Adults in the Netherlands". In: *International Journal of Human–Computer Interaction* 33.5 (May 2017), pp. 410–422. ISSN: 1044-7318. DOI: 10.1080/10447318.2016.1254890. URL: https://www.tandfonline.com/doi/full/10.1080/10447318.2016.1254890.

[158] Alessandro Acquisti and Ralph Gross Ralph. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook". In: *Privacy Enhancing Technologies*. Vol. 4258. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006. Chap. chapter 3, pp. 36–58. ISBN: 978-3-540-68790-0. DOI: 10.1007/11957454_3. URL: http://link.springer.com/10.1007/11957454_3.

[159] Christoph Lutz and Pepe Strathoff. "Privacy Concerns and Online Behavior–Not So Paradoxical After All? Viewing the Privacy Paradox Through Different Theoretical Lenses". In: *SSRN* (2014).

[160] Sanjeev Dhawan, Kulvinder Singh, and Shivi Goel. "Impact of Privacy Attitude, Concern and Awareness on Use of Online Social Networking". In: *Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-*. Vol. 2014. IEEE, Sept. 2014, pp. 14–17. ISBN: 978-1-4799-4236-7. DOI: 10.1109/CONFLUENCE.2014.6949226. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6949226.

[161] Hatoon S Alsagri and Saad S Alaboodi. "Privacy Awareness of Online Social Networking In Saudi Arabia". In: *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*. IEEE, 2015, pp. 1–6.

[162] Hanna Krasnova and Natasha F Veltri. "Behind the Curtains of Privacy Calculus on Social Networking Sites: The study of Germany and the USA". In: *10th International Conference on Wirtschaftsinformatik*. 2011, pp. 891–900.

[163] Mohamed Norshidah and Ahmad Ili Hawa. "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia". In: *Computers in Human Behavior* 28.6 (), pp. 2366–2375.

[164] Ashish Gupta and Anil Dhami. "Measuring the Impact of Security, Trust and Privacy in Information Sharing: A Study on Social Networking Sites". In: *Journal of Direct, Data and Digital Marketing Practice* 17.1 (Sept. 2015), pp. 43–53. ISSN: 1746-0166. DOI: 10.1057/dddmp.2015.32. URL: http://link.springer.com/10.1057/dddmp.2015.32.

[165] Shi-Woei Lin and Yu-Cheng Liu. "The Effects of Motivations, Trust, and Privacy Concern in Social Networking". In: *Service Business* 6.4 (Dec. 2012), pp. 411–424. ISSN: 1862-8516. DOI: 10.1007/s11628-012-0158-6. URL: http://link.springer.com/10.1007/s11628-012-0158-6.

[166] Anil Dhami et al. "Impact of Trust, Security and Privacy Concerns in Social Networking: An Exploratory Study to Understand the Pattern of Information Revelation in Facebook". In: *Advance Computing Conference (IACC), 2013 IEEE 3rd International*. IEEE, Feb. 2013, pp. 465–469. ISBN: 978-1-4673-4529-3. DOI: 10.1109/IAdCC.2013.6514270. URL: http://ieeexplore.ieee.org/document/6514270/.

[167] Naresh .K Malhotra, Sung S Kim, and James Agarwal. "Internet Users' Information Privacy Concerns (IUIPC): the Construct, the Scale, and a Causal Model". In: *Information Systems Research* 15.4 (Dec. 2004), pp. 336–355. ISSN: 1047-7047. DOI: 10.1287/isre.1040.0032. URL: http://pubsonline.informs.org/doi/abs/10.1287/isre.1040.0032.

[168] Eva-Maria Zeissig et al. "Online Privacy Perceptions of Older Adults". In: *International Conference on Human Aspects of IT for the Aged Population*. Springer, 2017, pp. 181–200.

[169] Sigal Tifferet. "Gender Differences in Privacy Tendencies on Social Network Sites: A Meta-Analysis". In: *Computers in Human Behavior* (2018).

[170] Ontsi. *Estudio Sobre la Ciberseguridad y Confianza en los Hogares Españoles*. 2018.

[171] Irwin Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Pub. Co., 1975. ISBN: 9780818501685.

[172] Sandra Petronio. *Boundaries of Privacy: Dialectics of Disclosure*. Suny Press, 2002.

[173] Minyue Ni et al. "An Empirical Study on User Access Control in Online Social Networks". In: *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*. SACMAT '16. Shanghai, China: ACM, 2016, pp. 13–23. ISBN: 978-1-4503-3802-8. DOI: 10.1145/2914642.2914644.

[174] Ghazaleh Beigi et al. "Securing Social Media User Data: An Adversarial Approach". In: *Proceedings of the 29th on Hypertext and Social Media*. HT '18. Baltimore, MD, USA, 2018, pp. 165–173. ISBN: 978-1-4503-5427-1. DOI: 10.1145/3209542.3209552. URL: http://doi.acm.org/10.1145/3209542.3209552.

[175] idp. *Gpen Privacy Sweep 2017 Finds Ambiguity in Privacy Policies*. 2017. URL: http://www.idp.al/2017/10/25/gpen-privacy-sweep-2017-finds-ambiguity-in-privacy-policies/.

[176] Amanda Nosko et al. "Examining Priming and Gender as a Means to Reduce Risk in a Social Networking Context: Can Stories Change Disclosure and Privacy Setting Use When Personal Profiles Are Constructed?" In: *Computers in Human Behavior* 28.6 (Nov. 2012), pp. 2067–2074. ISSN: 07475632. DOI: 10.1016/j.chb.2012.06.010. URL: https://linkinghub.elsevier.com/retrieve/pii/S0747563212001604.

[177] Ai Ho, Abdou Maiga, and Esma Aïmeur. "Privacy Protection Issues in Social Networking Sites". In: *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE, May 2009, pp. 271–278. ISBN: 978-1-4244-3807-5. DOI: 10.1109/AICCSA.2009.5069336. URL: http://ieeexplore.ieee.org/document/5069336/.

[178] Lærd. *Reliability in Research | Lærd Dissertation*. 2019. URL: https://bit.ly/2q1K4B5.

[179] Jum Nunnally. "Psychometric Theory—25 Years Ago and Now". In: *Educational Researcher* 4.10 (1978), pp. 7–21.

[180] Robert F DeVellis. *Scale Development: Theory and Applications*. Vol. 26. Sage Publications, 2016.

[181] George Darren and Paul Mallery. *SPSS for Windows Step By Step: A Simple Guide and Reference*. Boston: Allyn & Bacon, 2003.

[182] Manuela Farinosi and Sakari Taipale. "Who Can See My Stuff?: Online Self-Disclosure and Gender Differences on Facebook". In: *Observatorio (OBS*)* 12 (2018).

[183] Lærd. *Pearson Product-Moment Correlation*. 2019. URL: https://bit.ly/1LTbv1a.

[184] Statsoft. *How To Find Relationship Between Variables, Multiple Regression*. 2019. URL: http://www.statsoft.com/textbook/multiple-regression.

[185] Lærd. *Independent t-test for Two Samples*. 2019. URL: https://statistics.laerd.com/statistical-guides/independent-t-test-statistical-guide.php.

[186] Ronald W Rogers. "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation". In: *Social psychophysiology: A sourcebook* (1983), pp. 153–176.

[187] Darren Quinn, Liming Chen, and Maurice Mulvenna. "Does Age Make a Difference in the Behaviour of Online Social Network Users?" In: *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, Oct. 2011, pp. 266–272. ISBN: 978-1-4577-1976-9. DOI: 10.1109/iThings/CPSCom.2011.86. URL: http://ieeexplore.ieee.org/document/6142274/.

[188] Monika Taddicken. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure". In: *Journal of Computer-Mediated Communication* 19.2 (Jan. 2014), pp. 248–273. ISSN: 10836101. DOI: 10.1111/jcc4.12052. URL: https://academic.oup.com/jcmc/article/19/2/248-273/4067550.

[189] "A Survey of Social Media Users Privacy Settings and Information Disclosure". In: *The Proceedings of 14th Australian Information Security Management Conference*. 2016, pp. 67–75.

[190] Erving Goffman. *The presentation of self in everyday life*. Doubleday: Garden City, 1959. ISBN: 9780385094023.

[191] Bas Hofstra and Rense Corten and Frank van Tubergen. "Understanding the Privacy Behavior of Adolescents on Facebook: the Role of Peers, Popularity and Trust". In: *Computers in Human Behavior* 60 (July 2016), pp. 611–621. ISSN: 07475632. DOI: 10.1016/j.chb.2016.02.091. URL: https://linkinghub.elsevier.com/retrieve/pii/S0747563216301546.

[192] Gaurav Bansal and David Gefen. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online". In: *Decision support systems* 49.2 (May 2010), pp. 138–150. ISSN: 01679236. DOI: 10.1016/j.dss.2010.01.010. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167923610000230.

[193] C Nathan DeWall et al. "Narcissism and Implicit Attention Seeking: Evidence from Linguistic Analyses of Social Networking and Online Presentation". In: *Personality and Individual Differences* 51.1 (July 2011), pp. 57–62. ISSN: 01918869. DOI: 10.1016/j.paid.2011.03.011. URL: https://linkinghub.elsevier.com/retrieve/pii/S0191886911001310.

[194] Gaurav Bansal, Fatemeh Mariam Zahedi, and David Gefen. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online". In: *Information & Management* 53.1 (Jan. 2016), pp. 1–21. ISSN: 03787206. DOI: 10.1016/j.im.2015.08.001. URL: https://linkinghub.elsevier.com/retrieve/pii/S0378720615000853.

[195] Robert Glancy. *Will you read this article about terms and conditions? You really should do | Robert Glancy*. 2014. URL: https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information.

[196] Facebook. 2018. URL: https://www.facebook.com/.

[197] Facebook. 2019. URL: https://newsroom.fb.com/company-info/.

[198] Yoshinori Matsunobu. *Semi-Synchronous Replication at Facebook*. 2014. URL: http://yoshinorimatsunobu.blogspot.com.es/2014/04/semi-synchronous-replication-at-facebook.html.

[199] Data Center Knowledge. *The Facebook Data Center FAQ*. 2016. URL: http://www.datacenterknowledge.com/the-facebook-data-center-faq/.

[200] Kate Conger. *The Facebook Data Center FAQ*. 2016. URL: https://techcrunch.com/2016/07/08/messenger-adds-end-to-end-encryption/.

[201] Facebook. *Messenger Secret Conversations*. Tech. rep. Facebook, July 2016. URL: https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf.

[202] Facebook. *Statement of Rights and Responsibilities*. 2018. URL: https://www.facebook.com/legal/terms.

[203] Aliza Rosen. *Tweeting Made Easier*. Nov. 2017. URL: https://blog.twitter.com/official/en_us/topics/product/2017/tweetingmadeeasier.html.

[204] Peter Schuller. *Manhattan, our real-time, multi-tenant distributed database for Twitter scale*. Apr. 2014. URL: https://blog.twitter.com/2014/manhattan-our-real-time-multi-tenant-distributed-database-for-twitter-scale.

[205] Caitlin Dewey. *Ellen DeGeneres' Oscar selfie broke Twitter, and world records*. Mar. 2014. URL: https://wapo.st/2Zsxa1X.

[206] Twitter. *Request to verify an account | Twitter Help Center*. 2018. URL: https://support.twitter.com/articles/20174631.

[207] Twitter. *Privacy Policy*. May 2018. URL: https://twitter.com/en/privacy.

[208] Jon Russell. *Prominent Twitter Accounts Compromised After Third-Party App Twitter Counter Hacked*. Mar. 2017. URL: https://techcrunch.com/2017/03/15/twitter-counter-hacked.

[209] Jaiku archive. *Google acquires Jaiku*. 2007. URL: https://web.archive.org/web/20071225101821/http://jaiku.com/help/google.

[210] Bradley Horowitz. *A fall sweep*. Oct. 2011. URL: https://googleblog.blogspot.com.es/2011/10/fall-sweep.html.

[211] S. Wikipedia. *Google Services: Google Chrome, Youtube, Google Maps, Gmail, Google Books, Google Street View, List of Google Products, Orkut, Chromium, Gmail Interfa*. General Books, 2013. ISBN: 9781230570822. URL: https://books.google.es/books?id=O2gvNYaQciUC.

[212] tumblr. 2018. URL: https://www.tumblr.com/login.

[213] Statista. *Cumulative total of Tumblr blogs from May 2011 to April 2019 (in millions)*. Apr. 2019. URL: https://www.statista.com/statistics/256235/total-cumulative-number-of-tumblr-blogs/.

[214] Yahoo! *Yahoo! to Acquire Tumblr*. 2013. URL: https://investor.yahoo.net/releasedetail.cfm?releaseid=765892.

[215] tumblr. *European Privacy Policy*. 2018. URL: https://www.tumblr.com/privacy/en_eu.

[216] Todd Hoff. *Tumblr Architecture - 15 Billion Page Views A Month And Harder To Scale Than Twitter*. Feb. 2012. URL: http://highscalability.com/blog/2012/2/13/tumblr-architecture-15-billion-page-views-a-month-and-harder.html.

[217] MariaDB. *Tumblr uses MariaDB for multi-source replication*. 2018. URL: https://mariadb.com/kb/en/mariadb/tumblr-uses-mariadb-for-multi-source-replication/.

[218] tumblr. *Tumblr Privacy Policy*. 2018. URL: https://www.tumblr.com/policy/en/privacy.

[219] tumblr. *Tumblr Staff*. 2013. URL: https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had.

[220] Plurk. 2018. URL: https://www.plurk.com/portal/.

[221] Alexa. *plurk.com Traffic Statistics*. 2018. URL: http://www.alexa.com/siteinfo/plurk.com.

[222] pump.io. 2018. URL: http://pump.io/.

[223] identi.ca. 2018. URL: https://identi.ca/.

[224] JoinDiaspora*. 2018. URL: https://www.joindiaspora.com/.

[225] wikipedia. 2018. URL: https://en.wikipedia.org/wiki/Diaspora_(social_network).

[226] DiasporaFoundation. 2018. URL: https://diasporafoundation.org/.

[227] Gordon Morehouse. 2018. URL: https://joindiaspora.com/posts/2fdcda606b2c0133cd8b2adb80a2c223.

[228] Indrajeet Singh et al. "Twitsper: Tweeting privately". In: *IEEE Security Privacy* 11.3 (May 2013), pp. 46–50. ISSN: 1540-7993. DOI: 10.1109/MSP.2013.3.

[229] twister. 2018. URL: http://twister.net.co/.

[230] Miguel Freitas. "Twister: the development of a peer-to-peer microblogging platform". In: *International Journal of Parallel Emergent and Distributed Systems* 31.1 (Jan. 2016), pp. 20–33. DOI: 10.1080/17445760.2015.1053808.

[231] Miguel Freitas. *twister-a P2P microblogging platform*. 2013. eprint: 1312.7152.

[232] trsst. 2018. URL: http://www.trsst.com/.

[233] GitHub. 2018. URL: https://github.com/TrsstProject/.

[234] trsst. *Trsst: a secure and distributed blog platform for the open web*. Tech. rep. trsst, Aug. 2013. URL: http://www.trsst.com/paper/.

[235] GitHub. Mar. 2014. URL: https://github.com/TrsstProject/trsst/wiki/Frequently-Asked-Questions.

[236] Gab. 2018. URL: http://gab.ai.

[237] Gab. *Happy Birthday, Gab: Announcing Our Plans For An ICO*. Aug. 2018. URL: https://medium.com/@getongab/happy-birthday-gab-announcing-our-ico-e338662d26a1.

[238] Gab. 2018. URL: https://gab.ai/pro.

[239] Andrew Torba. *Andrew Torba on Gab*. Sept. 2017. URL: https://gab.ai/a/posts/12463989.

[240] Alan Dreyfus. *GAB.AI bans first user*. Jan. 2017. URL: http://www.1776again.com/2017/01/26/gab-ai-bans-first-user/.

[241] Gnu Social. 2018. URL: https://gnu.io/social/.

[242] Gnu Social. 2018. URL: https://gnusocial.net/doc/faq.

[243] World Wide Web Consortium. 2018. URL: https://www.w3.org/community/ostatus/wiki/Main_Page.

[244] Sonja Buchegger et al. "PeerSoN: P2P Social Networking: Early Experiences and Insights". In: *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*. SNS '09. Nuremberg, Germany: ACM, 2009, pp. 46–52. ISBN: 978-1-60558-463-8. DOI: 10.1145/1578002.1578010.

[245] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. "Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network". In: *2009 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks Workshops*. Kos, Greece: IEEE, June 2009, pp. 1–6. DOI: 10.1109/WOWMOM.2009.5282446.

[246] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. "Safebook: A privacy-preserving online social network leveraging on real-life trust". In: *IEEE Communications Magazine* 47.12 (Dec. 2009), pp. 94–101. ISSN: 0163-6804. DOI: 10.1109/MCOM.2009.5350374.

[247] Leucio Antonio Cutillo, Refik Molva, and Melek Önen. "Safebook: A distributed privacy preserving Online Social Network". In: *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*. Lucca, Italy: IEEE, June 2011, pp. 1–3. DOI: 10.1109/WoWMoM.2011.5986118.

[248] Daniel R. Sandler and Dan S. Wallach. "Birds of a FETHR: Open, Decentralized Micropublishing". In: *Proceedings of the 8th International Conference on Peer-to-peer Systems*. IPTPS'09. Boston, MA: USENIX Association, 2009, pp. 1–1. URL: http://dl.acm.org/citation.cfm?id=1855663.1855664.

[249] Timothy Perfitt and Burkhard Englert. "Megaphone: Fault Tolerant, Scalable, and Trustworthy P2P Microblogging". In: *2010 Fifth International Conference on Internet and Web Applications and Services*. Barcelona, Spain: IEEE, May 2010, pp. 469–477. DOI: 10.1109/ICIW.2010.77.

[250] Kalman Graffi et al. "LifeSocial.KOM: A P2P-Based Platform for Secure Online Social Networks". In: *2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P)*. Delft, Netherlands: IEEE, Aug. 2010, pp. 1–2. DOI: 10.1109/P2P.2010.5569977.

[251] Peter Druschel and Antony Rowstron. "PAST: a large-scale, persistent peer-to-peer storage utility". In: *Proceedings Eighth Workshop on Hot Topics in Operating Systems*. Elmau, Germany: IEEE, May 2001, pp. 75–80. DOI: 10.1109/HOTOS.2001.990064.

[252] Kalman Graffi et al. "LifeSocial.KOM: A secure and P2P-based solution for online social networks". In: *2011 IEEE Consumer Communications and Networking Conference (CCNC)*. Las Vegas, USA: IEEE, June 2011, pp. 554–558. DOI: 10.1109/CCNC.2011.5766541.

[253] Tianyin Xu et al. "Cuckoo: Towards Decentralized, Socio-aware Online Microblogging Services and Data Measurements". In: *Proceedings of the 2Nd ACM International Workshop on Hot Topics in Planet-scale Measurement*. HotPlanet '10. San Francisco, California: ACM, 2010, 4:1–4:6. ISBN: 978-1-4503-0177-0. DOI: 10.1145/1834616.1834622.

[254] Tianyin Xu et al. "Scaling Microblogging Services with Divergent Traffic Demands". In: *Middleware 2011: ACM/IFIP/USENIX 12th International Middleware Conference*. Lisbon, Portugal: Springer Berlin Heidelberg, Dec. 2011, pp. 20–40. ISBN: 978-3-642-25821-3. DOI: 10.1007/978-3-642-25821-3_2.

[255] Amre Shakimov et al. "Privacy, Cost, and Availability Tradeoffs in Decentralized OSNs". In: *Proceedings of the 2Nd ACM Workshop on Online Social Networks*. WOSN '09. Barcelona, Spain: ACM, 2009, pp. 13–18. ISBN: 978-1-60558-445-4. DOI: 10.1145/1592665.1592669.

[256] Amre Shakimov et al. "Vis-Vis: Privacy-preserving online social networking via Virtual Individual Servers". In: *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*. Bangalore, India: IEEE, Jan. 2011, pp. 1–10. DOI: 10.1109/COMSNETS.2011.5716497.

[257] DPCS. *Garlanet*. 2011. URL: http://dpcs.uoc.edu/projects/garlanet/.

[258] Emiliano De Cristofaro et al. "Hummingbird: Privacy at the Time of Twitter". In: *2012 IEEE Symposium on Security and Privacy*. San Francisco, California, USA: IEEE, May 2012, pp. 285–299. DOI: 10.1109/SP.2012.26.

[259] Emiliano De Cristofaro et al. "Tweeting with Hummingbird: Privacy in Large-Scale Micro-Blogging OSNs." In: *IEEE Data Eng. Bull.* 35.4 (2012), pp. 93–100.

[260] Sonia Jahid et al. "DECENT: A decentralized architecture for enforcing privacy in online social networks". In: *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. Lugano, Switzerland: IEEE, Mar. 2012, pp. 326–332. DOI: 10.1109/PerComW.2012.6197504.

[261] Sonia Jahid, Prateek Mittal, and Nikita Borisov. "EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation". In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ASIACCS '11. Hong Kong, China: ACM, 2011, pp. 411–415. ISBN: 978-1-4503-0564-8. DOI: 10.1145/1966913.1966970.

[262] Shirin Nilizadeh et al. "Cachet: A Decentralized Architecture for Privacy Preserving Social Networking with Caching". In: *Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies*. CoNEXT '12. Nice, France: ACM, 2012, pp. 337–348. ISBN: 978-1-4503-1775-7. DOI: 10.1145/2413176.2413215.

[263] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption". In: *2007 IEEE Symposium on Security and Privacy (SP '07)*. Oakland, California, USA: IEEE, May 2007, pp. 321–334. DOI: 10.1109/SP.2007.11.

[264] Jörg Daubert et al. "Twitterize: Anonymous Micro-blogging". In: *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*. Doha, Qatar: IEEE, Nov. 2014, pp. 817–823. DOI: 10.1109/AICCSA.2014.7073285.

[265] Jörg Daubert. "Anonymous Publish-Subscribe Overlays". PhD thesis. Darmstadt, Germany: Darmstadt, Technische Universität Darmstadt, 2016.

[266] George Pallis, Demetrios Zeinalipour-Yazti, and Marios D. Dikaiakos. "Online Social Networks: Status and Trends". In: *New Directions in Web Data Management 1*. Berlin, Germany: Springer Berlin Heidelberg, 2011, pp. 213–234. ISBN: 978-3-642-17551-0. DOI: 10.1007/978-3-642-17551-0_8.

[267] Ching-man Au Yeung et al. "Decentralization: The future of online social networking". In: *W3C Workshop on the Future of Social Networking Position Papers*. Vol. 2. Barcelona, Spain: W3C, 2009, pp. 2–7.

[268] Chi Zhang et al. "Privacy and security for online social networks: challenges and opportunities". In: *IEEE network* 24.4 (July 2010), pp. 13–18. ISSN: 0890-8044. DOI: 10.1109/MNET.2010.5510913.

[269] Sonja Buchegger and Anwitaman Datta. "A case for P2P infrastructure for social networks-opportunities & challenges". In: *Sixth International Conference on Wireless On-Demand Network Systems and Services*. Snowbird, UT, USA: IEEE, 2009, pp. 161–168.

[270] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. "Multiparty access control for online social networks: model and mechanisms". In: *IEEE transactions on knowledge and data engineering* 25.7 (2013), pp. 1614–1627.

[271] Andreas Krause and Eric Horvitz. "A utility-theoretic approach to privacy in online services". In: *Journal of Artificial Intelligence Research* 39 (Nov. 2010), pp. 633–662. DOI: 10.1613/jair.3089.

[272] *PDCA*. 2019. URL: https://en.wikipedia.org/wiki/PDCA.

[273] Victor R. Basili. *Software Modeling and Measurement: The Goal/Question/Metric Paradigm*. Tech. rep. College Park, MD, USA: University of Maryland at College Park, 1992.

[274] Victor R. Basili. "Applying the Goal/Question/Metric paradigm in the experience factory". In: *Software Quality Assurance and Measurement: A Worldwide Perspective* 7.4 (1993), pp. 21–44.

[275] R Van Solingen et al. *Goal Question Metric (GQM) Approach*. 2002.

[276] Rini van. Solingen and Egon Berghout. *The goal/question/metric method: a practical guide for quality improvement of software development*. The McGraw-Hill Companies, 1999.

[277] Borja Sanz et al. "A threat model approach to attacks and countermeasures in on-line social networks". In: *In Proceedings of the 11th Reunion Espanola de Criptografıa y Seguridad de la Información (RECSI)* (2010), pp. 343–348.

[278] Yong Wang and Raj Kumar Nepali. "Privacy threat modeling framework for online social networks". In: *2015 International Conference on Collaboration Technologies and Systems (CTS)*. IEEE, 2015, pp. 358–363.

[279] Samia Oukemeni, Helena Rifà-Pous Helena, and Joan Manuel Marquès Puig. "Privacy Analysis on Microblogging Online Social Networks: A Survey". In: *ACM Comput. Surv.* 52.3 (June 2019), 60:1–60:36. ISSN: 0360-0300. DOI: 10.1145/3321481. URL: http://doi.acm.org/10.1145/3321481.

[280] Prachi Kumari et al. "Distributed data usage control for web applications". In: *Proceedings of the first ACM conference on Data and application security and privacy - CODASPY 11* (2011). DOI: 10.1145/1943513.1943526.

[281] Elena Kozhemyak. "Privacy considerations for secure identification in social wireless networks". MA thesis. Royal Institute of Technology, 2011. URL: https://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2011/rapporter11/kozhemyak_elena_11116.pdf.

[282] Mohammad Badiul Islam. "Privacy by design for social networks". PhD thesis. Queensland University of Technology, 2014.

[283] Jayprakash Lalchandani and Hari Bhaskar Sankaranarayanan. "Risk Weighted Social Trust Index for Online Social Networks". In: *Procedia Computer Science* 78 (2016), pp. 307–313.

[284] Yahya Farashazillah. "A Security Framework to Protect Data in Cloud Storage". PhD thesis. University of Southampton, 2017. URL: https://eprints.soton.ac.uk/415861/1/Final_Thesis.pdf.

[285] Isabel Wagner and Eerke Boiten. "Privacy Risk Assessment: From Art to Science, by Metrics". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2018, pp. 225–241. ISBN: 978-3-030-00305-0. DOI: https://doi.org/10.1007/978-3-030-00305-0_17.

[286] OWASP. *Open Web Application Security Project: OWASP Risk Rating Methodology*. 2019. URL: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[287] OWASP. *OWASP Top 10 Privacy Risks Project*. 2019. URL: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project.

[288] NIST. "SP 800-30r1. Guide for Conducting Risk Assessments". In: *NIST* (2012). URL: https://bit.ly/2wRhgxN.

[289] NIST. "SP 800-53r4. Security and Privacy Controls for Federal Information Systems and Organizations". In: *NIST* (2013). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[290] CVE. *Common Vulnerabilities and Exposures (CVE)*. 2019. URL: https://cve.mitre.org/.

[291] E. Aghasian et al. "Scoring Users' Privacy Disclosure Across Multiple Online Social Networks". In: *IEEE Access* 5 (2017), pp. 13118–13130. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2720187.

[292] Ann Cavoukian. "Privacy by design: The 7 foundational principles". In: *Information and Privacy Commissioner of Ontario, Canada* 5 (2009).

[293] Nicholas Vollmer. *Article 35 EU General Data Protection Regulation (EU-GDPR)*. 2018. URL: http://www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm.

[294] Commission Nationale de l'Informatique et des Libertés. *Privacy Impact assessment (pia)*. Accessed: 26-June-2019. 2018. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.

Universitat Oberta de Catalunya
September 2019