# Privacy in Social Networks and Instant Messaging

## Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: von Mettenheim Vorname: Walter

[redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 27. 6. 2014

# Directory

# 1 Introduction

Everyday people all over the world make use of social networks and messaging services. In 2014 at least 1.8 billion people are members of social networks (Firsching, 2012). The amazing figure of at least 1.28 billion is part of the ultimate top dog: Facebook (n-tv, 2014). No wonder, as social networks offer a huge amount of possibilties: We can utilise them for information, communication, entertainment, education as well as to display our private and professional life. They have thus become an indispensable life-enhancing application. Generally, users don't have to pay cash for enjoying the convenience of social networks. But, of course, the offer of social networks and messaging services is not really free: Users provide something incredibly valuable – data.

In the first quarter of 2014 Facebook made a total revenue of 2.56 billion dollars (n-tv, 2014). Now, the crucial issue is to have a closer look at the origin of these revenues. Users generate extensive, detailed and profound personal information of unprecedented quality. The key is smart commercialization of this data. Therefore, not only the material directly provided is used. Social networks also employ indirectly available information like selected contents. This amount of data can be employed for advertising - and this kind of promotion is, of course, much more purposeful than classical advertising. Many social networks take further steps. They reserve their right to sell the collected data. Potential purchasers are other social networks and messaging services but also economic entities outside the social network industry and even government institutions like intelligence services (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2012). Moreover, the data is not only available to interested parties willing to pay: Depending on the privacy configuration every member has the ability to view the provided contents and potentially use them to the detriment of a user. On top of that, unauthorized access and in this context especially data theft is a further source for causing harm to a user.

It is crystal clear that the usage of social networks is a double-edged sword. Users can benefit a lot from diversified facilities provided by social networks. Even the usage of collected data by the social network provider or another stakeholder can possibly be advantageous for the user if it is not misused. On the other hand, of course, the provided data is of interest for plenty of stakeholders who might not use it in support of the user. Thus, the question arises:

***Which advantages and disadvantages could result for users from divulging private information in social networks and messaging services?***

And how can users as well as social network operators avoid misuse of data? Probably, most users are not aware of the extent to which their data is used, so, there seems to be some kind of asymmetric information. In order to draw attention to this fact, a German supermarket offered customers the opportunity to pay with their data (Boschmann, 2014), as depicted in Illustration 1. However, assessing the value of user's data or action is so important that social networks have even developed sophisticated methods for that purpose.


*Illustration 1: „Datenmarkt" in Hamburg, Germany*

*Source: (Boschmann, 2014)*

This paper is organized as follows. In section 2 basic information is provided, in section 3 a market research is done. Section 4, the main part investigates advantages and disadvantages of divulgation of private data and messaging services as well as evildoers' methods and protection mechanisms. It is followed by results, policy recommendation, discussion and conclusion.

## 2 Basic information

### 2.1 Defining Social Network & Instant Messaging

#### *2.1.1 Social Network*

The history of Internet based social networks dates back to the middle of the 1990s. Early social media sites like (still operating) classmates.com focused on bringing users together by sharing contact information (classmates.com, n. y.), while others such as theglobe.com featured the possibility to publish one's own personalized online content and to basically connect with people having similar interests (theglobe.com, 2009). Modern social networks can be seen as a convergence of „personal presenting" and „contacting": Social networks nowadays offer at least a user profile, the establishing of social links as well as a messaging service (Ellisson, 2007).

Within this Bachelor thesis it was not considerate that a user shall circumscribe the data he divulges on social networks and messaging services. It was rather assumed that a user publishes to his heart's content data of any kind and in any amount. This accomplished fact was assumed as fixed variable from which measures have to be divulged. However, paper review show that often questions like privacy-utility tradeoffs are investigated. This can go so far that a user shall seriously limit the amount of data he publishes to a very restrictive amount (Fire, et al., 2014). So, in this cases the bottom line is that a quiet contrary approach was chosen.

Possibly commercial solutions in order to protect oneself from the disadvantages could have been investigated in a deeper way. But it has to be noticed that in many papers already contained finished frameworks with all commercial software solutions were presented. So this issue is already fully investigated further research is hence of minor interest.

In the context of the policy recommendation advantages in social networks and messaging services (e. g. the providing of music services) not directly accruing from the divulgation of private data stay disregarded. Anyway, these other advantages could in the users' eyes consider a further value, balancing the disadvantages. Hence, there could possibly be a contortion to the con of the advantages. Also the quantitative evaluation with points is questionable. It is disputable, if the evaluation with a point system is adequate. On the other hand, the compiling of decision matrices is commonly recommended for decision processes in private as well as in scientific life. It is necessary for comparing different abstract factors. It might be considered as a bad method but is however the best one available.

# 9 Conclusion

Core question of this bachelor thesis where the advantages and disadvantages accruing from divulgation of private data on social networks. To this purpose a literature research was conducted in which the seven main advantageous features recommendation services, social connection services, services enhancing organization of community events, smart spaces, services enhancing data network connection, enhanced Advertisement and enhanced search queries based on users' preferences expressed on social networks were carved out. These services were subsequently classified in Maslow's hierarchy of needs. Thereby it could be asserted that generally, all kinds of needs can be fulfilled by social networks, but the basic physical needs as well the need for love and belonging can be fulfilled in a very strong way. As a counterpart in the following step the disadvantages were explored. As a result, five main disadvantages identity theft, social engineering focusing on influencing users' buying patterns,

uncovering asymmetric information, cyber bullying, stalking and sexual harassment as well as burglary and other non-sexual crimes were detected. These disadvantages were adjudged having negative impact on users' security, especially the financial and emotional security. On top of that, an overview of the methods evildoers apply for harming users and possible protection techniques was given. Protection techniques can be applied on the users' as well as on the social network operator's side. It thereby came out that a user can reduce his vulnerability by applying the protection methods, but a 100% shelter cannot be assured. Moreover, the methods demand a sacrifice in terms of effort, time and sometimes even money. Therefore, social network operators shall setup protection mechanism. All in all, it was reached the conclusion that any user should decide in dependence of subjective factors if he is ready to provide private data on social network or not.

Within this bachelor thesis several further questions for investigating arose. As implementing privacy protection methods are a strain it could be explored which is exactly the necessary amount of privacy, in this context the burglar example is to be point out. Furthermore, in terms of economics it could be inquired if the users' are actually aware of all privacy threats or if asymmetric information is on hand. Moreover, in terms of social sciences an enhancement of the very mathematical decision matrix could be conducted.

All in all, it can be ascertained that the divulging of private data on social networks and messaging services can supply the user with many advantages – until an evildoer comes into play. But users are not powerless. They can protect themselves. Actually, users as well as social networks can determine by their conduct if the divulging of private data is used to the advantage or the disadvantage of a user.

## Table of Literature

Acquisti, A. & Gross, R., 2011. Faces of facebook: Privacy in the age of augmented realit. *BlackHat USA*.

Ahmed, A. et al., 2014. Event-Based Mobile Social Networks: Services, Technologies, and Applications. *IEEE Access*, pp. 500 - 513.

Ahmed, J. & Shaikh, Z., 2011. Privacy issues in social networking platforms: comparative study of facebook developers platform and opensocial. *2011 International Conference on Computer Networks and Information Technology (ICCNIT)*, pp. 179 - 183.

Aimeur, E. & Schonfeld, D., 2011. The ultimate invasion of privacy: Identity theft. *2011 Ninth Annual International Conference on Privacy, Security and Trust*, pp. 24 - 31 .