



UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

A privacy dashboard for social networks

MASTER THESIS
FACULTY OF ECONOMICS AND SOCIAL SCIENCES

ANGELO GUGLIELMETTI

November 2017

Thesis supervisors:

Dr. Agnes Lisowska Masson

Pr. Dr. Denis Lalanne

Abstract

Social networks have acquired a huge popularity in the last ten years. A considerable amount of information is collected and shared constantly and can lead to problems and misunderstandings if shared with the wrong parties. That's why protecting and managing the social network users' privacy, for example by understanding and using the provided privacy settings, is of primary importance.

This work first analyzes the existing literature on the topic, finding a general lack of awareness and understanding of the privacy settings as well as a general difficulty using them.

The privacy settings and policies of five social networks are analyzed to see what choice is offered to the users and data about swiss university students' awareness and management of privacy on social networks is collected, obtaining results that confirm the findings of the literature review and therefore indicate difficulties in the privacy management and a lack of awareness about the default privacy settings offered by the different social networks.

Three interfaces for a prototype Privacy Dashboard, a web application to provide extended information about privacy settings and publicly shared content on a user's social networks and help managing the privacy settings are then developed. The usability and usefulness of the tool are tested by performing remote usability tests with 18 participants testing all three interfaces. No statistically significant difference is found concerning the performance and ease of use of the three tested interfaces. The majority of users find the tool very informative and report having learned something new about privacy on social networks and being interested in using such a tool if publicly available.

Keywords: Social networks, Dashboard, Privacy, Settings, Facebook, Twitter, LinkedIn, Google+, Pinterest.

Table of Contents

1 Introduction	1
1.1 Problem description	1
1.2 Analyzed Social networks	2
1.3 Objectives	3
1.4 Methodology and structure	4
2 Literature review	5
2.1 Privacy and personal information	5
2.2 Privacy settings management and awareness	7
2.3 Evolution over time	8
2.4 Existing privacy management tools.....	9
3 Social network sites analysis	12
3.1 Privacy policy	12
3.1.1 Facebook	13
3.1.2 Twitter	15
3.1.3 LinkedIn	16
3.1.4 Google +.....	18
3.1.5 Pinterest.....	20
3.2 Default settings	22
3.3 Heuristic evaluation	23
3.3.1 Facebook	23
3.3.2 Twitter	26
3.3.3 LinkedIn	27
3.3.4 Google +.....	29
3.3.5 Pinterest.....	31
3.4 Chapter Discussion	32
4 Testing awareness and difficulty perception – exploratory study	34
4.1 Introduction.....	34
4.2 Methods (survey structure and tools)	34
4.2.1 Questions	34
4.2.2 Participants	37

4.3	Results.....	37
4.4	Discussion.....	40
4.5	Survey limitations	42
5	Developing and testing a prototype	43
5.1	Requirements	43
5.2	Technical specifications.....	44
5.3	Interfaces overview.....	45
5.3.1	Interface 1 – Tabs	45
5.3.2	Interface 2 – Tiles.....	46
5.3.3	Interface 3 – Columns	47
5.4	Test	48
5.4.1	Method	49
5.4.2	Results	51
5.4.3	Discussion and future development	57
5.4.4	Limitations of the prototype and the test.....	59
6	Conclusion	61
7	References	63
8	Appendices	66
A	Default privacy settings	1
B	Survey Questionnaire (Chapter 4)	8
C	Survey results (SPSS / Excel output).....	26
D	Prototype test wizard screens.....	42
E	Test tasks	55
F	Prototype screens	58
G	Prototype test results (SPSS output)	67
H	Source Code.....	108

List of Figures

Figure 1: Screenshots of Facebook's Data Policy	15
Figure 2: Screenshots of LinkedIn's privacy policy	18
Figure 3: Screenshot of Pinterest privacy policy	21
Figure 4: Default privacy settings openness	22
Figure 5: Facebook privacy shortcuts, before and after	24
Figure 6: Privacy settings - tagging.....	24
Figure 7: Twitter privacy settings - Save button at the bottom of the page	26
Figure 8: LinkedIn mobile website	28
Figure 9: Google + settings	30
Figure 10 : Screenshot of the first interface	46
Figure 11 : Screenshot of the second interface	47
Figure 12 : Screenshot of the third interface	48
Figure 13: Screenshot of the list of tasks to accomplish on the test wizard.....	50
Figure 14: Subjective ease of use of every interface.....	54
Figure 15: Ease of comparison between social networks per interface	55

List of Tables

Table 1: Social networks privacy management tools.....	11
Table 2: Heuristic evaluation notation	23
Table 3 : Privacy policy structure elements	33
Table 4 : Social network usage frequency	38
Table 5 : Links to the four web applications used for the test	44
Table 6: Average time to finish an interface test	52
Table 7: Average percentage of successfully completed tasks	52
Table 8: Pairwise comparisons - Time to complete a "privacy policy" task.....	53
Table 9: Pairwise comparisons - Time to complete a "comparison" task	53
Table 10: Average user evaluation per interface.....	54
Table 11: Average evaluation for comparing information between social networks	55

1

Introduction

1.1 Problem description

Social networks are nowadays used by a great number of people all over the world and their use is expected to continue increasing [1]. A huge amount of information is generated and shared on these services every day. With such a great quantity of personal data circulating on social networks and potentially available to anyone, the users risk to find themselves exposed to several threats.

Spam, insurance discrimination, financial fraud, stalking, identity theft, pedophilia and sexual crimes[2][3][4] are only some examples of possible threats that could arise from the uncontrolled sharing of information on social network sites.

Furthermore, the information shared on these platforms, if seen by the wrong people or taken out of context, could cause issues and unwanted situations to the people sharing it. In the offline world, people tend to act differently depending on the context they are in. For instance, a college student will probably act differently when at a party with friends than he would when meeting with his grandparents or with a potential employer during a job interview [5]. It's relatively easy to differentiate the different contexts in the offline world, since the public seeing these multiple behaviors is there, physically present and clearly identifiable. That's not the case for social networks: if not managed correctly, the information uploaded could be seen by anyone, without the user knowing or realizing it.

That's why the management of one's privacy on social networks, for example by using the privacy settings, is of primary importance. Users need to be aware of what they are doing and of the ways they have to control and protect their private sphere on these online services.

1.2 Analyzed Social networks

Five different social networks have been selected to be part of this work. The services have been chosen so that they differ either according to their topic, their audience or the kind of information that is shared:

- Facebook is the most used social network in the world with 2 billion users as well as in Switzerland with 3.8 million users [6]. Every user creates a profile filled with personal information and shares multiple types of content with friends and other users.
- Twitter is a very popular social network, that only allows its users to post short messages up to 140 characters, accompanied if necessary by photos or videos. The user profile contains little explicit information about the user.
- LinkedIn is a professional social network where the users publish information that is mostly work related and create a profile similar to an online resume where they list their education, work experience and skills.
- Google+ is a social network owned by Google and for which many people have an account only because they have registered to use one of the many services offered by the company, like Gmail or Google Docs [7].
- Pinterest is different from the rest as the users only post a collection of items and links that they have found around the internet. The personal profile doesn't contain any explicit personal information.

The following paragraph shortly introduces every chosen social network goal and function.

Facebook

Facebook is an online social network launched in 2004 and created by Mark Zuckerberg. The social network was initially only open to Harvard students and gradually increased its user base, constantly gaining new users and becoming now the most popular social network in the world, with more than 2 billion active users [8].

By creating a Facebook account, users create a personal profile containing at least name and a profile picture. If desired, the profile can be completed with a considerable amount of information, including for instance demographic information like age, location, sentimental situation, family members as well as various photos and photo albums, videos, status updates and much more. Users can connect with each other by becoming “friends”, granting this way mutual access to each other's profiles.

When logging on the website, users are redirected to their news feed, where they can see the various contents published by their friends and their respective connections. The service started as a web application and it now includes applications for many different platforms.

Twitter

Twitter is a news and microblogging service founded in 2006 where users have the possibility to publish and read short messages called “tweets”, limited to 140 characters in length. Other

than that, Twitter users can also post content like images, videos and links. In addition, users can decide to follow other users and therefore see their tweets on the main page, called feed, as well as interact with those messages by retweeting or commenting them.

Like Facebook, Twitter is available as a web application as well as a series of applications for a myriad of platforms.

Google +

Google plus is a social network service owned by Google, one of the biggest search engine companies in the world. Google+ users can create a personal profile containing various information in a manner very similar to Facebook and publish different content like status updates, photos, videos and other.

Like on Twitter, users have the possibility to follow others' profiles without having to ask for permission that is instead required for Facebook. Followers can be organized into circles, so that it's later possible to decide what content can be shown to which group of followers.

LinkedIn

LinkedIn is a professional networking social network launched in 2003 with the purpose of connecting business contacts, publishing offers for new positions, share resumes and research and apply for open positions.

LinkedIn users have the possibility to create a personal profile, where they can add professional related information like education, past and current jobs, skills, languages and so on. Users can connect to other people, called "connections" and share different contents. Unlike the previously cited social networks, LinkedIn is made for professional contacts and thus the published information is normally adapted to the context.

LinkedIn is available as a web application and has apps for different platforms.

Pinterest

Pinterest is a visual social bookmarking site that allows its users to publish and share contents called pins including photos, videos and links about topics they are interested in, personally created or found on the internet and organized into pin boards. Pinterest users can subscribe to other people's boards and thus see and follow what others publish. Users can interact with other people's pins by commenting and re-pinning.

Unlike the other social networks described above, Pinterest's goal is more about sharing content found on the internet that is of interest to the user and less about sharing personal information.

1.3 Objectives

The goal of the project is to raise awareness regarding privacy on social networks by researching and developing a prototype for a tool called Privacy Dashboard, that allows the users to keep an eye and inform themselves on the possible privacy settings of the different social networks they have an account for. The tool should help the users understand the different

privacy-related aspects of their account and make their management easier. The development of the tool should take into consideration the User Centered Design principles and the result should be tested with users to assess its usefulness and usability.

1.4 Methodology and structure

The thesis will start with a review of the current literature about privacy on social networks. After an introduction to the topic, this paper will explore the research about people's awareness and concern, followed by an analysis of the privacy policies, default privacy settings and usability for the chosen social networks.

The following chapter will try to determine if the results of the literature review correspond to the reality by the mean of a survey about privacy awareness, concern and literacy conducted on a sample of 87 people.

In the third chapter, multiple interfaces for a prototype for the privacy dashboard will be designed, implemented and tested with users to assess its usefulness and usability.

The work will finish with the discussion of the results and the conclusion.

2

Literature review

This chapter is going to analyze existing literature on the subject of privacy on social networks and its control by the users, to see the current state of research and the key issues tied to this topic. Specifically, it is going to highlight what information is shared on social networks, how users manage it and how aware and in control they are of the tools at their disposal.

2.1 Privacy and personal information

Privacy is a word that constantly appears in many different contexts and can take many different definitions depending on the situation. Hiranandani [9] tries to give a general idea of the concept:

“Simply put, most people expect that an individual’s behavior will not be observed, monitored, or recorded without the person’s consent. Besides, they expect that the information they divulge will be treated confidentially and not used in unexpected or malicious ways.”

According to the author, the main concept deriving from the different privacy definitions is the ability of an individual to grant permission to see and use the information concerning their personal life and therefore to control who can be able to acquire and store this information as well as the way this can be used and shared.

With the advancements in telecommunications technologies of the last two decades and the shift to the interactivity of Web 2.0, that allows online information consumers to become information producers, the possibilities to share personal information online grow constantly and with it the importance of being able to control it.

Some of the main actors in this context are social networks, that allow everyone to easily share any kind of personal information, either directly or indirectly. In fact, judging from the analysis of the social networks privacy policies in chapter 3, the information that can be produced and shared by an individual on social networks can be of two main kinds:

Information the user shares willingly

This kind of information is composed by everything that the user publishes on the social network, either publicly or privately, by writing or publishing it directly. This includes the information given when creating a user account, the published contents like text, pictures and

videos and the information generated by interacting with elements or users, like liking other people's contents or commenting them.

Information the user shares automatically

This kind of information is given automatically whenever a user interacts with the social network and can be of technical nature, like for instance the information about the devices and applications used to access the service as well as the interaction with it, or can be inferred by analyzing the users' behavior, like for example the topics a user likes the most or the groups of contacts they are more likely to interact with.

The information generated and shared by using the social networks could potentially be directed and used by several types of public that can be divided in the following three main groups:

- Other social network users

These are the other individuals that have created an account for the social network and have the possibility to perform the same actions. Many social networks give the user the option to connect to other users and create a network of contacts with whom the user can interact in diverse ways.

- The social network itself

The company creating and maintaining the social network is often able to see the information that is shared by the user as well as the information that is collected automatically.

- Third parties

Many social networks interact and share information with several external service providers and partners. These could include for example companies responsible for the analysis of the collected data or advertising companies that use the information to tailor and target advertisements to the likings of the user.

To be able to control all this information, the social networks provide the users with a series of settings that allow them to control who can see and interact with the shared information to a certain degree, depending on the specific service. Most of these settings normally concern the other social network users, while a limited set of them is dedicated to the relation with third parties. The relation with the provider of the social network is normally defined by a privacy policy, a document that the users should read and must agree to when creating a user account that defines what information the social network can collect and how this information can be treated. Privacy policies will be analyzed in greater detail in chapter 3.1.

Because of their business model, social networks tend to favor open settings, i.e. the settings that make the shared information visible by a greater number of social network users. [3] This will be highlighted in chapter 3.2. In fact, independently from their topic, most social network's primary function is to share content and visualize what other users have shared, which means that the more content is shared, the more attractive the social network becomes. On top of that, one of the main sources of income for this kind of service comes from advertisements they sell to external companies [5]. For example ads accounted for 98% of Facebook total revenue in the

second quarter of 2017 [10], making the personalization of advertisements using user data a great income opportunity.

Sharing personal information on social networks can lead to a series of different risks. On one side, information could be seen and used by malicious entities to cause different types of problems like sending spam, financial fraud [3], “identity theft and sexual offense against children”[4]. Furthermore, if seen by the wrong public, the private information shared on social networks could be used against the user, for example by an employer looking for information about a potential candidate for a job [4] or by an insurance company researching its clients and seeing information out of context, like in the example provided by Kuczerawy and Coudert [5]:

“In 2009 a Canadian lady lost her health benefits when her insurance company discovered ‘happy’ pictures of her on her Facebook profile. She was on a sick leave due to a long-term depression and following an advice of her doctor, she was trying to get engaged in fun activities. Pictures of her smiling on a beach in Cancun or during a night out were taken by her insurance company as a proof that she is no longer depressed and able to work.”

In fact, Kuczerawy and Coudert [5] explain that people tend to act differently in the offline world according to the situation and context they are in, trying thus to prevent their behavior in one context to influence another. For instance, people tend to act differently when out for drinks with close friends than when they are at work meeting with a client.

If taken out of context and seen by the wrong recipient, information shared online on social networks could lead to problems in the offline life of an individual.

2.2 Privacy settings management and awareness

Most social networks provide their users with a set of privacy settings, more or less granular depending on the particular social network, to allow their users to control the audience for the shared information and try to prevent the creation of situations like the ones cited above.

These settings however are only useful if the users can use them correctly and do so which, according to multiple studies, is not always the case.

In fact according to Liu and al. [11] users have trouble effectively using the provided privacy settings and are therefore not taking advantage of their functionality, since “*only a minority of users change the default privacy preferences on Facebook*”. On this subject, Kuczerawy and Coudert [5] report that only 20% of Facebook users ever modify any of their privacy settings and Kajtazi and al.[12] state that “*people sometimes do not employ privacy settings for their privacy management when they use the social networking sites*”.

Multiple studies, mostly about Facebook since it’s the most used and well known online social network, indicate that social networks users find it difficult to manage their privacy using the provided privacy settings. The multiple settings that have to be checked in order to correctly manage one’s information on these online services can be a “*significant mental burden for many users*” [11] that “*may have no sufficient knowledge and patience to tune them*” [3] and can therefore feel confused about their usage and the effects that they provide on their information’s privacy [5].

The confusion and insecurity about the different privacy settings can lead the users to commit mistakes when setting them and share information with the wrong audience. For example, Liu and al. [11] report that only 39% of the time the tuned privacy settings match the expectations of the users regarding their effect, leading most of the time to overexposure of the shared contents.

This result is confirmed by another study [13] that compared sharing intentions of a set of users with the actual public for the analyzed content and found that all of the participants had at least one sharing violation.

Even when used correctly, the restriction of the audience and the corresponding privacy of the shared information can constitute a tradeoff between the protection of the personal information and the utility of the social network, without the user being necessarily aware of it [3].

To be able to correctly manage their privacy, users need to be aware of the potential risks and the tools they have at their disposal as well as of the public that can see their information. In fact, visibility preferences for the contents that people share on social networks, just like privacy settings in general, are often considered a static element that people can set the first time and then forget. Because of the dynamic nature of social networks, where one's network of connections and the service itself are constantly changing and evolving, privacy and visibility cannot be considered this way. Like the author explains, “*[...] users typically share a large number of items on SNSs with a large number of contacts. As a consequence, it becomes increasingly difficult after a while to remember which contacts can see which personal items.*” [14].

Of course, although most people, once aware of the privacy settings, tend to use them to manage their privacy [14], it doesn't mean that they will for sure, but it lays the basis for allowing them to make an informed choice.

2.3 Evolution over time

In the last ten years, online social networks have greatly evolved, as well in user base as in functionality and sharing possibilities. It is then imaginable that users' behavior concerning the shared content and the corresponding privacy has evolved with it.

But how did this behavior change? Stutzman, Gross and Acquisti [15], in their research, have found that Facebook users in their dataset have shown a more privacy conscious behavior over time and have been limiting the public for the content they share more than they did when the social network first appeared.

This trend, however, was somewhat slowed down by some changes to the Facebook platform and interface itself [15]. The increase in functions and sharing possibilities offered by the social network have in fact increased the quantity of information that is being published online.

The study also discovered that, with an enhanced sensation of security and control over their privacy, users have tended to share more content with their connections, increasing the amount of information that is shared with entities like “[...] third-party apps, (indirectly) advertisers, and Facebook itself” without even knowing.

Interestingly, a study performed by the Pew Research Center [16] showed “*that over time, regular use of social media without any major negative experiences may lessen their concerns about sharing information.*”

This doesn’t mean that users stopped caring about their privacy on social network but instead that they probably don’t understand well enough the way their information is collected and used by the social networks. On top of that, a contradiction has been observed between what users say and do: they claim to be concerned about their privacy online but the actions they take don’t support this claim [16].

Furthermore, the report indicates that 48% of the participants to the study still manifest some difficulties in managing their privacy settings, showing that the problem is still relevant.

2.4 Existing privacy management tools

During the literature review, many different tools for the management and the awareness increase about privacy on social networks were encountered, many of which were offline or not working anymore at the time of checking (August 2017). Here are some examples:

Sharemenot

Sharemenot [17] is a Firefox and Chrome add-on that prevents social network sites from tracking the user on websites that contain some of their service elements, unless they explicitly click on them. It works on multiple social networks, including all five services considered in this report. The add-on doesn’t exist as a standalone tool anymore and has been integrated into another tool called Privacy Badger [18].

Facebook Privacy Watcher

Facebook Privacy Watcher (FPW) [19] is a Firefox and Chrome add-on, developed by the Center for Advanced Security Research Darmstadt and the Technical University of Darmstadt, that shows the degree of privacy of a user’s posts by overlaying a color corresponding to the chosen public and allows the user to quickly change it.

The Chrome extension doesn’t seem to be available anymore and the Firefox one cannot be installed because of certificate issues.

Disconnect for Facebook

Disconnect for Facebook [20] is a browser extension for Firefox, Chrome and Opera designed to stop Facebook from tracking the user’s movements on the visited webpages, similar to what “Sharemenot” does. The add-on seems to be only available for Firefox, as the other two pages present an error message.

AVG Privacyfix

AVG Privacyfix [21] is a mobile application and browser extension to analyze one’s social profiles and highlight privacy settings that are too open according to their evaluation. The tool has been discontinued in 2016 [22] [23].

PrivacyCheck

PrivacyCheck [24] is an online tool to analyze a user's Facebook profile to look for public information and highlight it using a color scheme to show what is visible to the public. A score out of 21 is given to indicate how private the user profile is. The tool is still available and working.

Mcafee social protection

Mcafee social protection [25] [26] is a tool to blur or block the photos that are shared on Facebook to only allow specific people to see them and prevent them from being shared or copied without permission. The tool was available as a Facebook and Android app, but is no longer available.

Friend Inspector

Friend inspector [12] [25] is an online game developed to raise awareness about privacy on Facebook and help the players learn about the different privacy settings in a playful manner. The game is not available anymore since it was based on version 1.0 of Facebook API, which is not supported anymore.

Terms of service: didn't read

Terms of service: didn't read (TOSDR) [28] is a browser extension that helps the user evaluate and summarize the main points of various websites, including social networks. The evaluation of social network sites is only partial, since they haven't been analyzed enough to provide a general evaluation score.

In the following table it can be seen that most of the presented tools are not online anymore or not working. It would seem like a good part of them were just developed during the writing of academic papers and that they have not been maintained after that.

Name	Type of application	Development goal	Social networks	Still available
Sharemenot	Browser add-on	Academic	All five	No
Facebook Privacy Watcher	Browser add-on	Academic	Facebook	No
Disconnect for Facebook	Browser add-on	Unknown	Facebook	Partially
AVG PrivacyFix	Browser add-on/ mobile app	Commercial	Facebook, Google+, LinkedIn	No
PrivacyCheck	Online tool	Unknown	Facebook	Yes
Mcafee social protection	Facebook / Android app	Commercial	Facebook	No
Friend inspector	Online game	Academic/raise awareness	Facebook	No

Terms of service: didn't read	Browser add-on	Unknown	Facebook, Twitter, Google+	Yes
----------------------------------	----------------	---------	-------------------------------	-----

Table 1: Social networks privacy management tools

3

Social network sites analysis

The previous section has researched the existing literature to assess the awareness and privacy literacy of the social network users.

This section is going to analyze and report various aspects of the social networks themselves. It will be divided into three main sections:

Privacy policy: a quick analysis of the privacy policy contents of every social network analyzed as well as its structure to see how readable it is from a user's point of view.

Default settings: an observation of the default values of the privacy settings offered by the different social networks, to see what a newly created (or never modified) user profile looks like in terms of privacy.

Heuristic evaluation: an analysis of how easy it is to find the privacy settings and to understand and change them. The analysis will include the desktop version of the social network website, as well as the web mobile version and the android application to see if there are any significant differences.

- Desktop website: 14" Lenovo laptop, Windows 10, Chrome browser.
- Mobile website: Samsung Galaxy S7 android smartphone (5,1" screen), Chrome browser.
- Android App: Samsung Galaxy S7 android smartphone.

The chapter will end with a summary of the findings and, if necessary, a brief comparison of the five considered social networks.

3.1 Privacy policy

The privacy policy is defined as follows by Business Dictionary [29]:

"Statement that declares a firm's or website's policy on collecting and releasing information about a visitor. It usually declares what specific information is collected and whether it is kept confidential or shared with or sold to other firms, researchers or sellers."

People often agree to this document without even reading it, because they trust the service provider to avoid doing anything that could harm their privacy or simply because they don't have time to read it. In fact, McDonald and Cranor [30] discovered that an average person would need to spend about 244 hours a year to read all the privacy policies of the services they use.

This chapter will analyze the privacy policies of the five concerned social networks, looking at the following aspects:

- Content: this section will see what the policy says about the information the social network can collect about the user, the way they can use it and the people and services this information can be shared with.
- Structure: this section will describe some technical and cosmetic properties of the privacy policies, like the length, measured in number of words by copy-pasting the content in MS Word and using it to get the total, and the type of language and terminology used, determined by personal observation.

3.1.1 Facebook

Content

Facebook collects a large quantity of information about their users [31]. In the first section of their privacy policy they explain that they collect information the users give them when using their services, ranging from the information given during the registration process to “*information in or about the content*” [31] that is provided, including also the information about how the users interact with the different services offered. Another source of information could be other users, as it is possible for Facebook to collect information that other people share with photos, messages or contact synchronization. Other information collected includes information about a user’s contacts and their interaction with them, as well as information about payment and shipping information if the service is used for financial transactions.

The list continues with the device information collected by the social network, which includes “*operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers*” as well as location determined using GPS, Bluetooth or WIFI and connection information like IP address, ISP, Browser; mobile phone number and language.

Moreover, Facebook also tracks the user and collects information whenever they visit external websites that use any Facebook services like for instance the like button or Facebook login. This information includes the visited websites or used apps and whatever the developer provides to them.

Finally, information about the user can be given to Facebook by third parties like advertisers, service partners or companies of the Facebook group, according to their respective privacy policies.

The privacy policy goes on by detailing the way the collected information is used. The first cited goal for this information is to personalize content and analyze the way the users interact with the service to be able to provide them with useful suggestions about people to connect with, people to tag in photos, tailor the services according to the user’s location to allow them to look for local events or information or to inform their friends that they are in the same area.

Other possible uses include communicating with the user about their services and their changes or answer possible questions as well as show personalized ads to the user and measure their performance. Lastly, the information that the company can collect can be used to verify accounts and their activity, investigate suspicious activities or possible violations of their terms of use.

The collected information can be shared with different publics according to its type and the context. Some information can be voluntarily shared with people the user shares and communicates with while other, according to the privacy settings, can be publicly available and seen by people on and off Facebook services as well as by API's. On top of that, the shared information could be downloaded and shared by other users.

The policy continues by explaining that some information can be shared with “*apps, websites and third-party integrations*” that are on or user some of Facebook services. This means that when using Facebook services on external resources, these entities could receive information like username and ID or, according to the permissions they ask, information about age, location, language, the user’s friends and other contents like the shared comments or data about their application’s usage.

On top of that, information that Facebook collects can be shared with companies that are part of the group as well as a possible new owner in case of acquisition and other third parties. These third parties include “*advertising, measurement and analytics services*”, that can obtain a series of non-personally identifiable information to personalize and run their services, and other vendors and partners necessary for the creation and maintenance of the offered services. Lastly, the user information could be shared with legal entities if required by the applying legislation.

Structure

Facebook data policy contains 2624 words. The policy (called data policy on the Facebook website) is divided into 8 main sections:

- What kinds of information do we collect?
- How is this information shared?
- How can I manage or delete information about me?
- How do we respond to legal request or prevent harm?
- How our global services operate
- How will we notify you of changes to this policy?
- How to contact Facebook with questions?

The different sections are well separated from each other, highlighted in distinct colors and navigable from the top of the page thanks to a table of contents showing the different sections’ titles as well as every paragraph inside them, as it can be seen in the following picture.

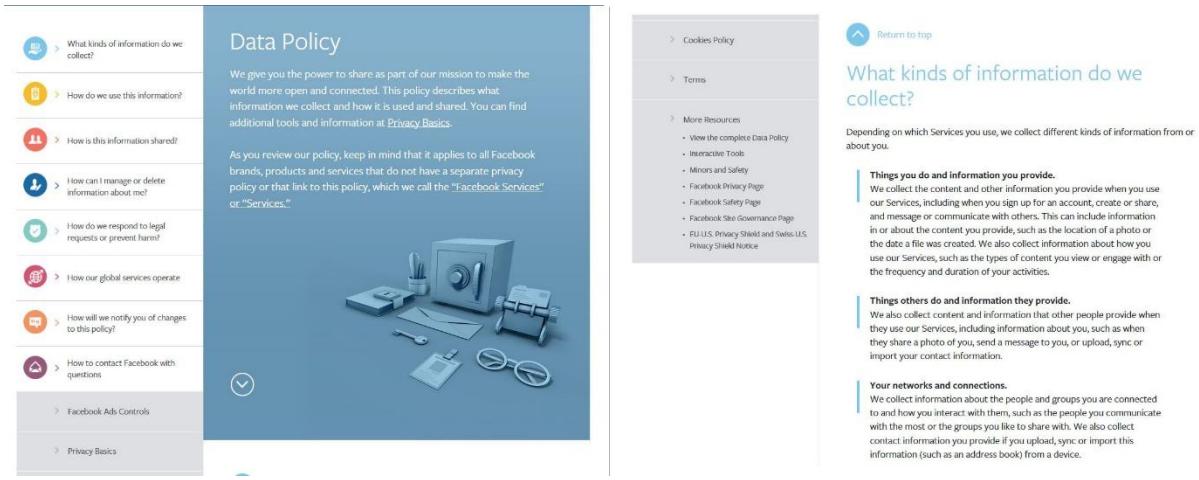


Figure 1: Screenshots of Facebook's Data Policy

The used language is easy enough for everyone to understand and the more general terms are explained using examples.

3.1.2 Twitter

Content

Unlike the other social networks' privacy policies, Twitter doesn't separate data collection from data usage and explains both in the same paragraphs.

Twitter collects various information from its users [32]. It starts with the basic information the users give when creating an account, like name, username, email address and password and explains how name and username are always publicly visible. It then goes on by explaining that the contact information like phone number and email address can be used to provide services like login verification or Twitter via SMS as well as to send information, to market, and to help other users and third-party services to find the user's account.

Additional information like the user's address book, if provided by the user, can be used to help find other users as well as to personalize the shown content according to the contacts in it. Other information could be collected from external services if the users connects them to the Twitter account and used to provide and improve the offered services.

Additional information that is given to the social network includes the profile data like description, date of birth or a picture, as the messages that are tweeted. On top of that Twitter collects technical information like the user interactions with the service, device information and location data, that can be used to make inferences with the goal of providing the user with personalized content and advertisements.

Information voluntarily shared by the user is public by default, but some of that information can be controlled using the provided privacy settings. The collected information can be seen and used by third parties like search engines, market research firms, application developers (if

they use a Twitter element). Because of the public nature of most of the information provided by the user, Twitter suggests thinking carefully before publishing something on their services.

Twitter can track the user when they interact with external services that use some Twitter element, by redirecting clicks or by using cookies stored on the user's machine. Since the last revision, Twitter no longer supports the "Do not track" feature of browsers. The user can now use a series of privacy controls on the Twitter website instead.

Logged data can be kept for a maximum of 18 months. After this period, it will be deleted or stripped of every "*common account identifiers*" like username, IP address, email address and others.

Structure

Twitter privacy policy contains 3453 words. The policy is structured as a long text, divided into four main sections:

- Information collection and use
- Information sharing and disclosure
- Accessing and modifying your personal information
- Our global operations

Every section is divided into smaller paragraphs, to make it easier to read. No table of contents is provided, so the only way to navigate the document is by scrolling along the page.

The language used for the document is easy to understand and only requires a minimal understanding of the service and the internet.

3.1.3 LinkedIn

Content

LinkedIn collects various data from its users [33]. Like on other social networks, LinkedIn privacy policy starts by explaining that they collect the information that is given by the user during the registration process, including email address, password and, if the user registers for the premium service, payment information. To this, is added the information that is voluntarily included in a user's profile. Here LinkedIn reminds the users to avoid posting or adding personal information that they wouldn't want to be available publicly.

Other information collected by the social networks includes the information that the users send when publishing something, participating to survey, apply for jobs, send invitations or import the user's address book as well as email headers and calendar information (including time, participants, places and contacts) if synced with the service.

They could obtain additional information from other users, when they post something concerning someone on LinkedIn or on one of their services, unless the users opt-out in the privacy settings, or sync their address book. Furthermore, data is collected and given to LinkedIn from partners like employers or applicant tracking systems.

Just like the other social networks, LinkedIn collect log data about the user interaction with the website and the different LinkedIn services as well as information about the interaction with external websites containing any LinkedIn element and technical data like IP address, website visited before and after the contact with LinkedIn content, browser and add-ons, carrier, ISP, proxy servers and location data.

The list of collected information continues with information about messages, including automatic scanning of the content, information provided by employers about employees using the service and other premium characteristics and information that could be collected in the future to provide new services.

The collected information is used for a myriad of different goals, first of which is to provide their services, suggest new connections and nearby contacts, personalize the suggestions and the news that are shown to the user, suggest new skills to learn or career opportunities and updating other users, according to the selected privacy settings.

The profile information can be found by users looking to hire or be hired and get information about others who work in the same company or industry or that have similar skills.

The provided information can also be used to provide premium users with search functionalities as well as to personalize the shown advertisements, to perform market and other types of research, to market and further develop their services, as well as to perform investigations about possible violations of their user agreement.

Information collected is shared with other users, according to the privacy settings and the service usage, with people that need to archive communications for legal reasons, service providers that the user liked to their profile, affiliates that help provide their services like maintenance and analysis partners, legal entities if considered necessary and possible new future owners.

Structure

LinkedIn privacy policy contains a total of 5011 words.

LinkedIn's privacy policy starts by explaining to the user the importance of being transparent about their collection and use of user data. Following this principle, they offer the user a short video where they explain what their privacy policy is and cite the main points, as it can be seen in the following figure.

Figure 2: Screenshots of LinkedIn's privacy policy

Thereafter, the privacy policy is organized in different sections, easily navigable through a table of contents at the top of the page, pointing to the following sections:

- Introduction
- Information we collect
- How we use your data
- How we share information
- Your choices & obligations
- Other important information

The language used to describe every point is not complicated and easily understandable by most common people who have at least an idea of the services offered by LinkedIn. The text is divided into short and easy-to-read paragraphs, with a key phrase resuming them on the right side of the page.

One thing to be noted is that in the paragraph talking about the information shared voluntarily by the user, it is specified to never publish sensitive information that one wouldn't want to be public, written bold to make it more easily noticed.

3.1.4 Google +

Contents

Google collects data about the users of its myriad of services in different ways [34]. The first source of user data is constituted by the data that the users give up voluntarily, for example when creating a Google account or completing the personal Google+ profile.

This information is complemented by what Google can get from the usage of its services. In fact, in the policy they explain that they can get information about the devices used to access the different services, like OS, device identifiers, mobile network information and mobile phone

number and associate them with the used account. Other examples of this kind of collected information are represented by many kinds of logs, for example usage details, telephony logs, device event information and more as well as by location information collected using the different sensors and connections available to the used device, and cookies created by the different websites that use Google services or by partner companies. All this information can be linked to a user's account.

According to the privacy policy, the collected information is used firstly to provide and maintain the different offered services, as well as for improving them and developing new ones. The document continues saying that the information can also be used to personalize the services to the users, for instance by providing "*more relevant search results and ads*" or by applying the name and photo on services requiring a Google account.

Other uses include displaying information on the user's personal profile if they created one, as well as communicating with the user in case of problems, adapt the content to the user, for example by automatically changing the interface language, or to run automated services like Google analytics.

The information collected by the different Google services can be aggregated in one account.

The collected information can be shared with several different entities. Examples include domain administrators, if they manage the account, affiliates responsible for the processing of the data, legal entities requiring it to comply with the applicable regulations, and entities inside of Google.

Sensitive personal information is not shared unless explicitly permitted by the user by opting-in to the corresponding options.

Structure

Google privacy policy contains 2828 words.

Google + doesn't have a privacy policy dedicated exclusively to the social network. Instead, a common privacy policy for all of Google services is used. This means that the contents of this document are much more general than the ones on the other social networks and therefore don't refer precisely to the different social networking functions of Google+.

The document is divided into 12 different sections:

- Information we collect
- How we use information we collect
- Transparency and choice
- Information you share
- Accessing and updating your personal information
- Information we share
- Information security
- When this privacy policy applies

- Compliance and cooperation with regulatory authorities
- Changes
- Specific product practices
- Other useful privacy and security related materials

The document is navigable through a table of contents at the top left of the page, containing the different sections' titles. When useful, the main sections are divided into smaller paragraphs to be more easily readable.

The language used is easy to understand but it's very general, because of the broad number of services that this privacy policy concerns. Many different terms are explained using examples that appear in small popup windows that appear when clicking on any underlined term.

3.1.5 Pinterest

Contents

Pinterest collects various information from its users, including information that the user gives up voluntarily or for which gives permission to the social network [35]. Specifically, the privacy policy names the following information:

Name, profile photo, Pins, comments, likes, email address or phone number used to sign up, location data. In case of a transaction, payment, contact and purchase information are also shared with the company. If the user gives permission to Pinterest to access their other social network accounts, the company can obtain information like the contacts from the other services, if the respective privacy settings allow it.

On top of the voluntarily given information, the service can get technical information when the user is on their services, like log data containing IP address, visited web pages using Pinterest elements, information about browser type and settings, date and time and information about how the user interacts with Pinterest. Cookie data can also be collected (their usage is detailed in a separated Cookies Policy) as well as device information like the type of device, the OS, device settings and identifiers.

The third way to collect data described in the policy concerns the information that the service obtains from partners and advertisers, including information about click through rates and information about targeting.

According to the privacy policy, the collected information is used to provide the services, improve them and “protect Pinterest and our users”. The information can be stored for later usage from the user, for example when saving payment information. Another use for this information is to customize content as well as advertisements. In fact, it can be used to show the user personalized pins and people suggestions, as well as ads regarding other objects they have bought on the platform. On top of that, Pinterest can use the information to send their users updates, newsletters and marketing material, depending on the selected account settings, and to help other users (including the ones from other connected services) find a specific profile.

The collected data can be shared with multiple entities depending on the kind of information and on the situation. The “public boards” can be viewed by anyone as well as through the use of the available API’s. Other services like Facebook and Twitter can access the user’s information if the Pinterest profile is linked with the corresponding profiles on those social networks. In case of commercial transactions, necessary payment and contact information can be shared with the sellers and is then regulated by the sellers’ own privacy policies. Other external companies that could have access to the data include third party companies that analyze the ads performance, financial companies that store and manage the payment information, security consultants and other non-specified third-party providers working on Pinterest’s behalf.

If considered necessary, information could be shared with legal entities as well as new owners or other partners or advertisers (non-identifiable information only for the latter).

Structure

Pinterest privacy policy contains 2240 words.

As it can be seen in the following picture, Pinterest privacy policy is made in a Q&A structure, where the text is divided in different sections according to their content:

- We collect information in a few different ways:
- How do we use the information we collect?
- Transferring your information
- What choices do you have about your information?
- How and when do we share information?
- Our policy on children’s information
- How do we make changes to this policy?
- How can you contact us?

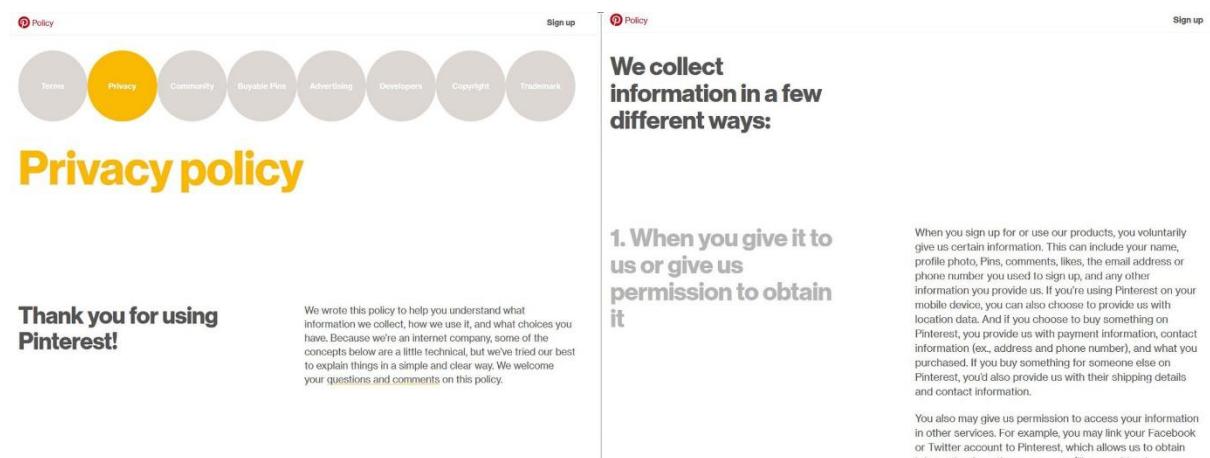


Figure 3: Screenshot of Pinterest privacy policy

Some sections, like the one about the ways the information is collected, are divided in different paragraphs, according to the type of information they focus on.

The language of the privacy policy is relatively easy to understand, as it doesn't contain any complicated law terms and it's written using everyday language. Some technical terms, like for instance "cookies" or "log" cannot be avoided but are explained using easy to understand examples.

3.2 Default settings

Chapter 2 has highlighted that, because of their business model, social networks tend to set the privacy settings to their most open values by default to maximize the amount of information that is shared on the platform.

To check if the problem was still actual, an analysis of the default privacy settings offered by the five considered social networks has been performed, observing the provided privacy settings and reporting what value was set by default. The value was considered open if it corresponded to the most open possibility amongst the available choices, private if the most private possibility was chosen and moderately private if the chosen value was in between the two extremes.

The following figure shows the results of the analysis. For a complete list of the privacy settings offered and their default values see appendix A.

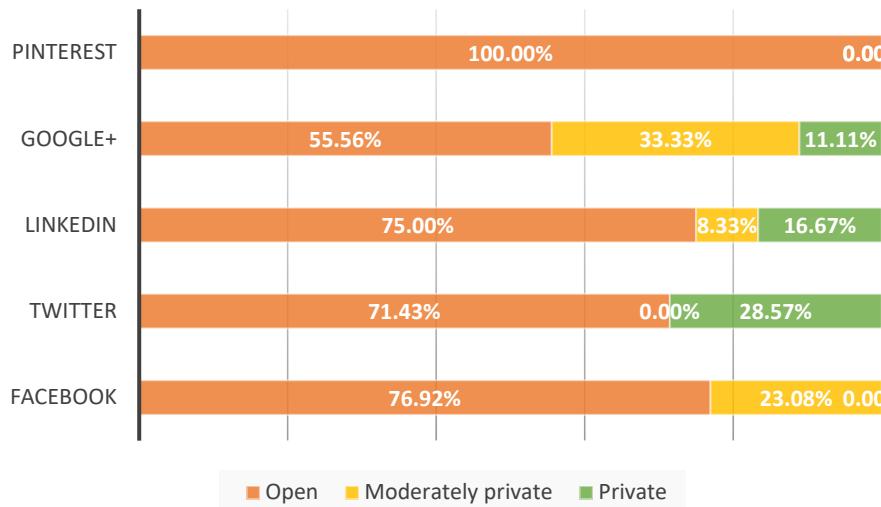


Figure 4: Default privacy settings openness

As it can be seen, the majority of social networks still favor the most open privacy settings available by default. The only exception is Google+, applying this principle only to 50% of the provided privacy settings. LinkedIn, Twitter and Google+ provide a small percentage of settings that are set to the most private possibility, while Facebook only provides a small quantity of moderately private default settings. This means that the social networks users cannot

count on the default privacy settings if they want to protect the information they share from overexposure.

3.3 Heuristic evaluation

After checking the privacy policies and the default settings for the five considered social networks, a short heuristic evaluation of the privacy management pages has been performed to assess how easy it is to find these pages and change the privacy settings. The analysis has been done on Desktop as well as mobile.

The following notation, described in the table below, has been used to report the problems found:

“[Type of error] (Severity) Description of the problem”

Type of error	The usability principle the problem refers to. The following 9 principles have been used for the analysis: <ol style="list-style-type: none">1. Simple and natural dialog2. Speak the user's language3. Minimize user's memory load4. Be consistent5. Provide feedback6. Provide clearly marked exits7. Provide shortcuts8. Deal with errors in a positive manner9. Provide help
Severity	The severity of the problem found, going from 1 (not really a usability problem) to 5 (Extremely important to fix).
Description	A textual description of the problem.

Table 2: Heuristic evaluation notation

3.3.1 Facebook

On Facebook, people have the possibility to set the audience for their content either by using the audience selector on the bottom of the input field for posting content or in the privacy settings page. For this reason, both have been analyzed.

Desktop web page

The usage of the audience selector on the Facebook desktop web page was generally easy and intuitive. The selector is positioned on the bottom left corner of the publishing window and a snippet of the selected audience helps identify its function. Once selected, the different options are easily identifiable and accompanied by an intuitive icon and a brief description.

- No particular usability problems were found for this element.

To access their privacy settings, the users previously (end 2016) had two possibilities: either use the privacy shortcut on the top right corner of the page, or go through the settings page. The former option has been moved in the help section and is therefore only visible if the user expands the help menu, accessible through an icon on the top right corner of the page, as it can be seen in the following image.

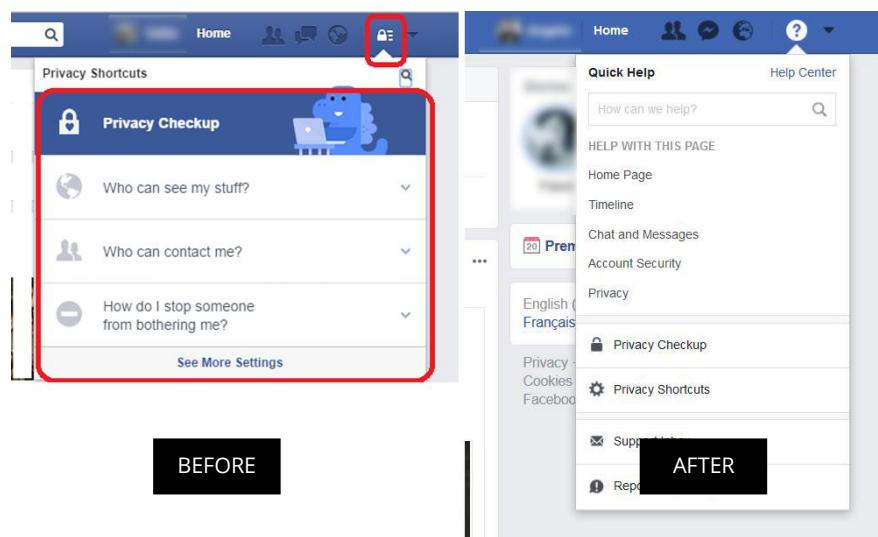


Figure 5: Facebook privacy shortcuts, before and after

Once the settings page accessed, the privacy section can be found on a list on the left of the page. It should be noted that not all privacy settings are in this section. In fact, additional settings concerning the tagging of people on pictures are in a separate section, as it can be seen in 6.

Timeline and Tagging Settings			
Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your Timeline?	Custom	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Custom	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Custom	Edit
Review	Who sees tag suggestions when photos that look like you are uploaded?	No One	Edit
	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review what other people see on your timeline.	View As	
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

Figure 6: Privacy settings - tagging

The settings are shown in a consistent way that provides feedback about the selected value and, when a setting name is not self-explanatory, provide a description with examples to illustrate its function.

No warning is displayed when the user selects a very open value, it's up to the user to be sure of what they are doing.

To summarize, this section presents the following problems:

- [2-3] (7) The shortcut to the privacy settings has been moved in a less visible menu. Users must actively look to find it.
- [2-3] (4) Not all privacy settings are in the privacy section.
- [1] (8) No warning is shown when a very open value like “public” is selected. This is arguably not a usability problem, but could be useful nonetheless.

Mobile web page

The audience selector is in the same position as on the desktop page and represented by a gear icon, showing that this is for setting something. When opened, the same list of possible values is shown, accompanied by the same icons but this time without the descriptions, probably because of space constraints. A checkmark indicated the selected value.

- Once again, no particular usability problems were found for this element.

The privacy settings can be accessed by tapping on the “sandwich” icon on the top right corner of the screen, and by selecting either the “Privacy Shortcuts” or “Account settings” items. Both items are towards the bottom of the list, the user must scroll to see them.

Once accessed, the settings are presented in the same order as on the desktop version and show the selected value below each label. The same short descriptions are provided when tapping on a setting.

- The same problems found in the desktop version can be applied here: not all the privacy settings are in the privacy section and no warning is shown when selecting an open value.

Android app

The audience selector on the android app works similarly to the mobile web version but is on top of the page instead of the bottom. The rest of its functions stays the same.

- [1] (4) Slight inconsistency between android app and mobile web version. More of a design choice than a usability problem.

The privacy settings can be accessed just like in the mobile web version, by tapping on the menu icon on the top left corner of the screen. The account settings item is situated towards the end of the list.

Once inside the “account settings” page, it works like in the mobile web version, just with differently styled icons.

- No additional usability problems were found on the android app.

3.3.2 Twitter

On Twitter, users can manage their privacy through the privacy settings page. Therefore, only this element has been analyzed.

Desktop web page

The Twitter privacy settings page can be accessed by clicking on the user profile image on the top right corner of the page and selecting “settings and privacy”. This is consistent with what can be found on many other services nowadays.

Privacy settings are presented as a well separated list and include a brief description when not self-explanatory. The selected value for each setting is clearly visible.

After changing a setting, the user must scroll to the end of the page to save the changes, like shown in Figure 7. Since the save button is not constantly visible, it could be easily forgotten and the changes to the privacy settings would not be saved. No warning is shown when exiting the page.

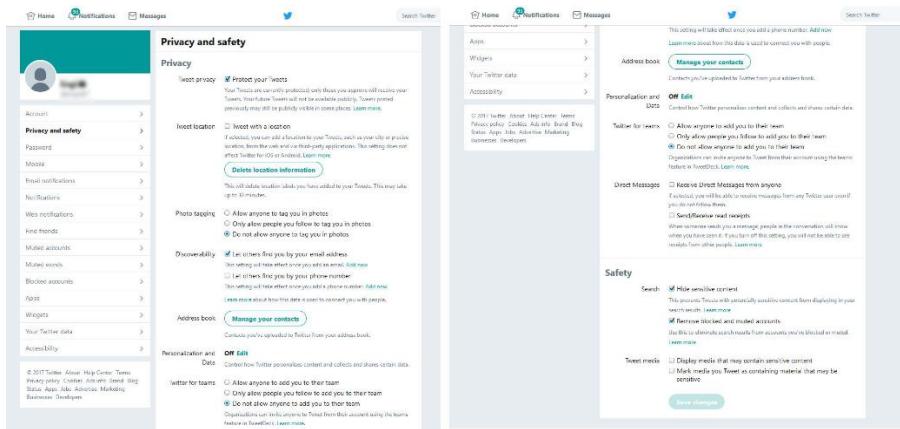


Figure 7: Twitter privacy settings - Save button at the bottom of the page

To summarize, this section presents the following problems:

- [4] (5-8) For the changes to take effect, the user must scroll to the end of the page and click the save button. If they forget to do it, no warning is shown. The save button should be always visible or, more conveniently, the changes to the privacy settings should be automatically saved as soon as they are selected.

Mobile web page

The privacy settings page on the mobile web version of Twitter can be accessed by tapping on the user profile image on the top left corner of the screen and by selecting “settings and privacy”, similarly to the desktop web version. On the list of settings, a brief description of the setting’s function is provided when not self-explanatory and the selected value is clearly visible.

The “Twitter for teams” setting is not present in the mobile web version and the remaining list is in a slightly different order than on the desktop. The settings are automatically saved when changed.

- [2] (4) The privacy settings order is not consistent with the desktop version. This could make a user think that some settings are not available since they are not where they are used to find them.

Android app

The privacy settings page on Twitter android app can be accessed by tapping on the menu icon on the top left corner of the screen and by selecting “settings and privacy”.

Once accessed, the list of settings is similar to the one presented in the mobile web version, but the settings concerning the discoverability of the profile through email address and phone address require an additional tap to enter the “Availability and contacts” section.

The rest of the page is similar to the mobile web version.

- [2] (4) The settings concerning the discoverability through email address and phone number are a bit hidden, compared to the other two versions. Adding them to the main list would make them more visible, without making it too long.

3.3.3 LinkedIn

Similarly to Facebook, LinkedIn allows to choose the public for a publication by using the audience selector on the publishing window or by going on the privacy settings page. These two sections will be analyzed.

Desktop web

The audience selector appears on the bottom of the page, right next to the “post” button when clicking on the publishing window. The selected audience is clearly visible and clicking on it displays the list of possible choices with a very short description below them.

- No particular usability problems were found for this element.

The privacy settings are accessible by clicking on the user’s profile image on the top right of the page and by selecting “settings and privacy” afterwards.

The different settings are divided into sections that can be navigated using a small index at the top left corner of the page.

A short description of the function of the settings is visible under each element and a more comprehensive one is displayed when clicking on it and contains a link to an external description page if necessary. The selected value is clearly visible.

- No particular usability problems were found for this element.

Mobile web page

The audience selector on the mobile web page is represented by a gear icon on the bottom left corner of the publishing screen, representing the post settings. Users must click on the icon to see who the audience for the post is.

- No particular usability problems were found for this element.

The privacy settings page can be accessed by tapping on the user profile image on the top left corner of the page, just under the different menu icons and by tapping on the gear icon in the top right corner afterwards. Since the profile image preview is very small, it looks like it could be easily missed, as it can be seen in the following picture.

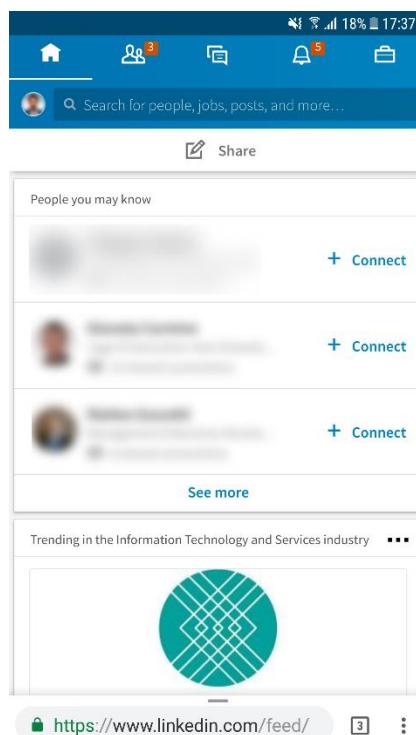


Figure 8: LinkedIn mobile website

The privacy settings are presented in a list, where every setting is followed by a short description of its function and displays a longer description when clicked. The selected value is not visible from the main list, the user must click on a setting to see it. Some settings are in a different order compared to the desktop version and the “Representing your organization” setting is missing on the mobile version.

To summarize, this section presents the following problems:

- [3] (1-2) The user’s profile picture is so small that it doesn’t look like something that can be clicked/tapped on a touchscreen phone. Making it slightly bigger or displaying it in line with the other sections would make it clearer.
- [2] (4) The privacy settings are on a different order than the desktop version. Having them in the same order would be more consistent.

- [3] (5) The value of every setting is not visible from the main list of privacy settings. It would be quicker if the user could see them without having to click on every single item.

Android app

The audience selector on the LinkedIn android app is similar to the one found on the mobile web page. One notable difference is in the icon that is displayed: a gear is shown to symbolize a setting of some kind, making it more intuitive.

- No particular usability problems were found for this element.

The privacy settings page can be accessed similarly to the mobile web page, by clicking on the user profile image, that is now in the top right corner of the page, above the other section icons. Just like on the mobile web version, the image is very small and doesn't really look like something that can be clicked/tapped on a touchscreen phone.

The list of settings is visually identical to the one presented on the mobile web version, including the missing feedback about the selected value for the settings. On top of that, some settings like "who can see your connections" or "notifying connections when you're on the news" are not included in the android app.

To summarize, this section presents the following problems:

- [3] (1-2) Just like in the mobile web version, the user's profile picture is so small that it doesn't look like something that can be clicked/tapped on a touchscreen phone. Making it slightly bigger or displaying it in line with the other sections would make it clearer.
- [3] (4) Only a selection of the privacy settings available on the web are manageable on the android app. This could preclude their management by android-only users.
- [3] (5) The value of every setting is not visible from the main list of privacy settings. It would be quicker if the user could see them without having to click on every single item.

3.3.4 Google +

On Google+, users have the possibility to change the visibility for their posts using the audience selector on the publishing window or by going into the privacy settings. These two sections will be analyzed.

Desktop web page

The audience selector is found on the top of the publishing window as a link saying "Choose people to share with" if nothing has been selected before, or the corresponding choice otherwise. Clicking on it displays the selected value as well as a "see more" item, needed to see the other possible choices. When selecting "public" a warning appears telling the user that by selecting that value they will allow people that are not in their circles to see and comment what they are sharing.

- [2] (7) The user needs to click twice to see the possible choices. Showing them directly would be quicker.

The privacy settings can be accessed by clicking on “settings” in the left menu. There is no specific section for privacy settings, all settings are put together in the settings page. A section is called privacy but only contains a link to clear the Google+ search history or go to the general Google settings, as it can be seen in Figure 9.

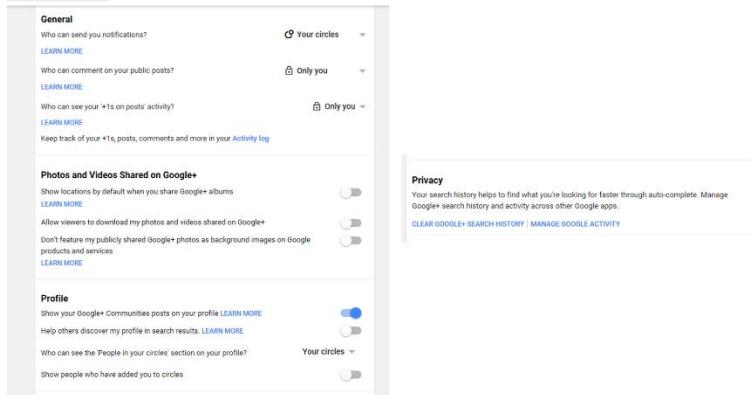


Figure 9: Google + settings

The settings are presented as a list with a link to a more comprehensive explanation. The selected value is clearly visible.

To summarize, this section presents the following problems:

- [3] (2) The settings are presented all together on the settings page. The privacy section only provides links to the Google general settings. This could be confusing for a user only wanting to manage their Google + privacy options.

Mobile web page

The audience selector on the mobile web page is identical to the one found on the desktop version, so the same comments apply.

The privacy settings page can be accessed by tapping on the menu icon on the top left corner of the page and on “settings” on the menu that appears on the left.

Once the page accessed, the users is presented with the exact same settings that can be found on the desktop version, visualized in the exact same way.

Once again, the same comments made for the desktop version apply.

Android app

The audience selector on the android app is located right under the user name on the publishing window. It shows the selected audience for the content. When clicked, a list of possible choices is directly displayed, unlike the web version where an additional step was required.

- No particular usability problems were found for this element.

The settings page is accessible by tapping on the menu icon on the top left corner of the screen and by selecting “settings” afterwards. If more than one Google account is registered on the smartphone, the user can select the one they want to change the settings for.

The settings are divided in a series of sections. Once again, the privacy section only contains links for clearing the Google + search history and to the general Google settings. Only a selection of the settings available on the web version are manageable here. For example, “who can comment on your posts” or “who can see the People in your circles section on your profile” are not present.

Once a section selected, the settings are displayed similarly to the web version, with a short description and, when necessary, a link to additional information.

- [3] (1-2) Like on the web version, the privacy settings are scattered between the rest of them and not in the existing privacy settings. More order is required.
- [3-4] (4) Only a selection of the privacy settings available on the web is visible on the android application. This could leave them unmanaged by users who only use the android app.

3.3.5 Pinterest

Pinterest privacy settings are manageable with the dedicated page. Only this element will be analyzed.

Desktop web page

The settings page can be accessed by clicking on the user’s name and profile picture on the top right side of the page, and on a bolt icon on the left afterwards. The settings related to privacy are not on a separate section. Every setting shows a brief description of its function as well as a link to get more information. The selected value/state is clearly visible. After changing a setting, the user must click a “save” button on the bottom of the page to make the changes effective. No warning is shown if the user tries to exit the page without saving.

- [2] (2) The privacy settings are not in a dedicated section. This is not extremely bad, since there are only three of them.
- [3-4] (5) For the changes to take effect, the user must click the save button. If they forget to do it, no warning is shown. The changes to the privacy settings should be automatically saved as soon as they are selected.

Mobile web page

Privacy settings are accessible by clicking/tapping on the “saved” section icon and on the bolt icon on the top left of the page afterwards. On the main page, the icon used to indicate is not consistent with the text that corresponds to it. In fact, the icon of a human shape is displayed, which normally indicates the user profile, but the “saved” label is attached to it, which could startle users that are not used to the website.

Once the page accessed, the settings are the exact same as on the desktop version, visualized in the exact same way.

To be effective, the changes to the settings must be saved using the button on the bottom of the page. The user must scroll all the way down for it, and it cannot be seen anyway since it is covered by the banner asking to install the android application.

- [4-5] (1) The save button has to be clicked to save the settings but it is covered by the banner asking to install the android application.

Android app

The privacy settings are accessible by clicking on the profile icon on the top right corner of the screen and on the bolt icon on the top right afterwards. Once opened, the list of settings is the same as on the web version and visualized in a very similar way, with a short description of their respective function and a toggle indicating their state. The changes are automatically saved.

- No particular usability problems were found for this element.

3.4 Chapter Discussion

In this chapter three privacy aspects of the five social networks have been analyzed: Privacy policy, default settings and ease of use of the privacy options (through a heuristic evaluation).

Social networks seem to have understood that privacy is an important component of their service and that the users are becoming more privacy conscious with time. In fact, the privacy policies of the analyzed social networks were mostly easy to read and were written in a language easily understandable by anyone with a minimal computer knowledge (like knowing what a browser is). Many concrete examples were given for the most general or complicated terms. Four out of five privacy policies were easily navigable using a table of contents with links to the different sections and every section was clearly separated by the others. The only exception was Twitter, as its privacy policy didn't provide a way to quickly navigate it. The only possibility is to scroll along the page. The longest privacy policy was LinkedIn's, while the shortest was Pinterest's. The majority of the policies were related directly to the social network and used examples from that context. The only exception was Google+, since its privacy policy is general and the same for all Google products. A summary table of the privacy policies' structure can be seen below.

	Facebook	Twitter	LinkedIn	Google +	Pinterest
Policy length (nr. of words)	2624	3835	5114	2883	2298
Well separated paragraphs	✓	✗	✓	✓	✓
Table of contents	✓	✗	✓	✓	✓

Understandable language	✓	✓	✓	✓	✓
Examples	✓	✓	✓	✓	✓

Table 3 : Privacy policy structure elements

Concerning the contents, all social networks collect diverse information about their users, mainly of the same type. In fact, they collect the information that the user gives voluntarily when creating an account or publishing content, log data about the user interaction with the website, information about the user given by other users when publishing content, technical data like used devices, IP address, carrier/ISP and others and data about the external websites containing a social network element that the user visits.

The information is used mainly to provide the offered services and to personalize the content that the user sees, depending on the type and topic of the social network. On top of that, user information can be used to personalize advertisements and to perform studies and aggregations.

Because of their business model, social networks tend to favor open privacy setting to increase the information that is shared by the users and with it the utility of the service they provide.

This is reflected by the default privacy settings provided at the creation of a new account. This is particularly true for Facebook and LinkedIn, where most of the privacy settings are set to the most open value by default. Twitter, Google+ and Pinterest were only moderately open, since many settings were set to an intermediate value, including remote connections but not the whole social network public.

Some exceptions were the settings that control the visibility of the profile from search engines, the personalization of the ads and the possibility to look for a user's account starting from the email address: these settings were open on all the social network but Pinterest.

Since the companies that offer the social networks services are big and surely have no shortage of competent personnel, one could think that all usability problems are assessed and taken care of before they hit the public. The performed heuristics evaluations have shown that, while this is mostly the case, there are still some aspects of the privacy settings usability that could be perfected. Most of these problems are in relation to the consistency between different version of the service, i.e. Desktop web page, mobile web page and mobile application. In fact, multiple social networks have decided to only offer a selection of the available privacy settings on their mobile web and application versions. The first explanation would be that some functions are not available on the mobile application and therefore don't need the corresponding privacy settings on that device, but the absence of some settings like "who can see your connections" on LinkedIn doesn't seem to relate to that.

In general, the desktop version of every social network is the better choice to manage a user's privacy settings, as it normally provides the complete list of settings. On more than one social network, the privacy settings were not grouped in a specific section.

4

Testing awareness and difficulty perception – exploratory study

4.1 Introduction

The previous chapter has observed the five social networks to see the content of their privacy policies, their default privacy settings and the ease of use of these settings.

This chapter will try to assess multiple perceived aspects of privacy on social networks by a set of swiss users. The goal is to discover how sure they feel about their control of their privacy on these services and the trust they put in the different service providers. This will allow to check what functions of the Privacy dashboard are relevant and should be implemented in the prototype that will be developed and tested in the following sections.

4.2 Methods (survey structure and tools)

The exploratory study was performed using an online survey, custom created using a tool called “Limesurvey” [36]. The survey was anonymous and was translated in four languages (EN, DE, FR, IT). It was usable on desktop as well as on mobile.

4.2.1 Questions

The survey included a total of 57 questions and was divided into the following six distinct sections. Only the fields concerning the social networks the user had an account for were displayed. The full set of questions of the used questionnaire can also be found in appendix B.

Demographic data:

A set of questions to assess the demographic characteristics of the participants as well as their use of the mentioned social networks.

- Gender
- Age range

- Occupation
- I have an account for the following social networks.

The user can select the social networks they have an account for, choosing between the five services analyzed in this paper and an additional field “other”.

- How often do you use these social networks?

The user can select one possibility for every social network they have an account for, going from hourly to daily, weekly, monthly and less often.

- What do you use the social network(s) for mainly?

The user should indicate what purpose they mainly use their social networks accounts for, choosing between stay in touch with friends, stay up to date with news and events, fill up spare time, share opinions, share photos and videos and other, with the possibility to specify.

Importance:

This group of questions has the purpose of assessing how important people consider their privacy information and the possibility to control its diffusion.

- I’m ok with giving personal information in exchange for a service.

The user indicates on a Likert scale if they consider acceptable to exchange their private information with a company for a provided service.

- It is important to know and be able to control who can see the information I share.

The user indicates on a Likert scale how important they consider having the possibility to manage and decide who can see the information they share.

- I’m concerned that the information I submit could be used for “commercial purposes”.

The user indicates on a Likert scale how concerned they consider themselves about the fact that their information can be used to target ads or be sold to third party companies with the same goal.

Control:

This group assesses the confidence of the users concerning their control over privacy on social networks as well as the frequency with which they check it.

- I know exactly who can see the information I share.

The users indicate on a Likert scale how confident they are that only the people they want can access and see the information they share on each of the social networks they have an account for.

- I carefully choose the public for the information I share every time I publish something.

The users indicate on a Likert scale if they take the time to check the audience for the contents they share when they post something on each social network they have an account for.

- The last time I reviewed my privacy settings was.

The users indicate when they last reviewed their privacy settings on a scale going from “last week” to “last month”, “last year”, “When I created the account”, “never” and “I don’t know” for each social network they have an account for.

- I’ve read the privacy policy of the following social networks

The users indicate the social networks of which they have read the privacy policy.

Trust:

This group assesses the trust that the users put in the social networks regarding their privacy.

- I trust the social network to choose the best default settings for the protection of my privacy.

The user indicates on a Likert scale if they think that the different social networks already sets the privacy settings to be conservative about the information that is shared.

- I am concerned that the information I publish on the social network could be misused.

The users indicate on a Likert scale if they fear that their information on each social network could be used for a purpose different from the one it is supposed to be used for.

Usability:

This group of questions tries to assess the perceived usability and clarity of the different privacy settings pages on the social networks analyzed.

- The privacy settings are easy to find.

The users indicate on a Likert scale if they consider it easy finding the privacy settings page on each of the used social networks.

- I understand what every privacy setting does.

The users indicate on a Likert scale if they think to understand the effect of every setting on the visibility and use of the information they share on each of the used social networks.

- I feel overwhelmed by the number of settings and I often think I forgot to set something important.

The users indicate on a Likert scale if the number of privacy settings offered by each social network make them feel overwhelmed is therefore not ideal.

- To manage my privacy settings, I prefer to use.

The users indicate what device they normally use to manage their privacy settings on each social network they use, choosing between “Website”, “mobile website” and “mobile app”.

Since not all settings are available on all platforms, the users that use exclusively the mobile application could miss some of them.

Default privacy settings:

The purpose of this question group is to check whether the users know what values are set by default when a new account is created. To do that, a comprehensive list of all the available

privacy settings on each of the used social networks is shown to the user. The respondents then choose the right setting between the available choices, that correspond to the ones offered on the respective websites.

4.2.2 Participants

Participants were recruited by word of mouth between friends and acquaintances on Facebook, as well as by writing to the mailing lists of the Joint Master in Computer Science (JMCS) and the computer science department of the Fribourg university.

A total of 87 completed questionnaires were received. The majority of participants were females (61%) students (70%) aged between 19 and 30 (85%) and took the survey in English (64%). On average, the respondents had an account for 2 of the 5 proposed social networks, one of which was almost always Facebook (95%).

4.3 Results

For the complete set of results, see appendix C.

Demographic data:

- Gender: Participants were divided into 61% females and 39% males
- Age range: 79% of participants were aged between 19 and 30 years old, while the remaining were divided between 31 to 50 (13%) and older than 50 (2%).
- Occupation: Most participants were students, either at the Fribourg university (48%) or elsewhere (22%). The remaining 30% indicated to have a different job.
- I have an account for the following social networks.

On average, the participants to the survey have an account for 2 to 3 social networks (Mean: 2.57, Std. deviation: 1.32), one of them being almost always Facebook (95%). Two of the participants said not to have an account for any social network because they don't want to share their personal information online. In fact, almost all the participants with at least an account for a social network (97.6%) have an account on Facebook while 60 to 70% of them have account for the other social networks (68.2% for Twitter, 63.5% for LinkedIn, 64.7% for Google+ and 70.6% for Pinterest). The frequencies of every combination can be seen in appendix C.

- How often do you use these social networks?

As it can be seen in the following table, Facebook is the most frequently used social network, with 67% of the users saying that they use it daily and 27% hourly. The other social networks are used less often, especially Google + and Pinterest.

	Facebook	Twitter	LinkedIn	Google +	Pinterest
Hourly	26.83%	3.70%	0.00%	0.00%	0.00%
Daily	67.07%	22.22%	16.13%	6.67%	12.50%
Weekly	3.66%	22.22%	45.16%	10.00%	25.00%
Monthly	0.00%	18.52%	25.81%	13.33%	20.83%
Less often	2.44%	33.33%	12.90%	70.00%	41.67%

Table 4 : Social network usage frequency

- What do you use the social network(s) for mainly?

The scope for the use of every social network obviously depends on its topic and audience. The participants indicated that they use Facebook mainly to “stay in touch with friends” (72.3%), “stay up to date with news and current events” (65.1%) and to “fill up spare time” (61.4%). Twitter is used to “stay up to date with news and current events” (66.7%) while LinkedIn is used to enlarge and maintain the network of professional contacts and look for a job (58.1%), Pinterest is used to look for ideas and inspiration (48%) and Google + is not really used, as a good part of the participants with an account for the social network of the search giant (50%) say that they only have an account because it was automatically created when registering for a general Google account and only 20% of them uses it to fill up spare time.

Importance:

- I'm ok with giving personal information in exchange for a service.

Most respondents say that are not ok with giving up their personal information to obtain a service. In fact, 40% disagree with the statements and an additional 21.2% strongly disagrees.

- It is important to know and be able to control who can see the information I share.

Most of the respondents agree (30.6%) or strongly agree (64.7%) on the importance of being in control of the public for the personal information that is shared on social networks.

- I'm concerned that the information I submit could be used for “commercial purposes”.

A big part of the participants (42.4% + 25.9%) feels concerned about the fact that their information could be used to personalize the advertisements that they see on the different social networks they visit.

Control:

- I know exactly who can see the information I share.

67% of the participants with a Facebook account is confident that they know the public that has access to the information they share on Mark Zuckerberg's social network. The situation is different for the other social networks listed in this paper. In fact, Twitter users have various levels of confidence on this matter, since only 44% of them claim to know more or less exactly who can see what they share (22.2% agree, 22.2% strongly agree) while the rest isn't sure (26%) or disagrees (30%).

On the remaining three social networks, roughly 40% of the participants (41.9% for LinkedIn, 34.3% for Google + and 40% for Pinterest) isn't sure and the rest is split between agree and disagree.

- I carefully choose the public for the information I share every time I publish something.

The majority of the participants with a Facebook account (77.2%) take the time to carefully choose the audience for their content every time they post something on the social network. A similar trend can be observed by Twitter users (59.2% agree/strongly agree). On LinkedIn, the results are more evenly distributed between “disagree” and “strongly agree”, while on the remaining social networks, most users are not sure (46.7% on Google +, 48% on Pinterest).

- The last time I reviewed my privacy settings was.

Virtually half of Facebook users (49.4%) answered that they had checked their privacy settings in the month preceding this survey and another 20.5% did that a year before the survey. Twitter users reviewed their privacy settings a year or even longer before the survey, while LinkedIn Google+, and Pinterest users only checked them when creating the account or never.

- I've read the privacy policy of the following social networks.

36.47% of Facebook users claim to have read the social network's privacy policy. Most other users (62.35%) say that they haven't read any of their social networks' privacy policies.

Trust:

- I trust the social network to choose the best default setting for the protection of my privacy.

Facebook users have a tendency not to trust the social network about choosing a set of default settings that helps protect their privacy. In fact, 73.5% of them don't agree with the statement. A similar trend, even if less drastic, can be observed between Twitter users, since 52.8% of them disagrees with the statement and another 18.5% is not sure. LinkedIn users are a little more trusting, with 41.9% of them trusting the professional social network and 22.6% being not sure.

On Google+ and Pinterest the respondents are not sure or disagree with the statement.

- I am concerned that the information I publish on the social network could be misused.

Facebook users are once again the most concerned about the possibility of their information being used for goals different from the ones it is intended: 69.9% of them agree or strongly agree with this statement. On Twitter, LinkedIn and Google + roughly 40% of the users consider themselves concerned about this possibility and 20 to 35% of them are not sure. On Pinterest, the majority of the users (52%) are not sure and only a total of 28% is concerned about the problem.

Usability:

- The privacy settings are easy to find.

Most Facebook users (74.7%) consider the privacy settings easy to find. On the other social networks, most people are not sure, except for LinkedIn, where the majority of users is split between “Agree” and “not sure”.

- I understand what every privacy setting does.

45.8% of Facebook users agree on the fact that they understand what every privacy setting does on the social network, while the rest is either not sure (21.7%) or disagrees (32.5%). Twitter and LinkedIn users show a similar trend, while the users of the remaining social networks are mainly not sure.

- I feel overwhelmed by the number of settings and I often think I forgot to set something important.

47% of Facebook users agree or strongly agree when asked if they feel overwhelmed by the number of privacy settings that they have to manage. On Twitter, Google+ and Pinterest users are mostly not sure while on LinkedIn are split between “not sure” and “disagree” (32.3% each).

- To manage my privacy settings, I prefer to use.

The majority of the users (66 to 87%) prefers to use the desktop website of their respective social networks to manage their privacy settings while some prefer to use the mobile application (13 to 32%). Almost no one uses the mobile website to accomplish this task.

Default privacy settings:

The participants to the survey were presented with a list of the privacy settings that they would find on the social networks for which they have an account and asked to fill in the values that they believed to be the default ones, chosen when a new account is created with no intervention from the user. The results were then compared with the actual defaults taken from the different social networks to see what percentage of the users’ choices corresponded and if the mistakes indicated a more strict or public default value.

The results were similar for the five social networks. In fact, the users scored an average around 50% of right answers (48% for Facebook with std.dev. 0.21, 50% for Twitter with std.dev 0.11, 49% for LinkedIn with std.dev. 0.19, 44% for Google+ with std.dev 0.13 and 57% for Pinterest with std.dev 0.44).

In most cases, the users that didn’t indicate the right default value thought that the default setting would be stricter than it actually was (76% on Facebook, 56% on Twitter, 85% on LinkedIn, 67% on Google+ and 52% on Pinterest).

4.4 Discussion

The participants to the survey have accounts on multiple social networks. Facebook is by far the most popular between them, even though the others have pretty high account rates too. Having an account for a social network does not imply active use though: in fact, many Google+ users reported that they only have an account because they have created a Google account and that they never use the social network. Facebook is the only social network that is used at least daily by the majority of its users.

The results show that most users tend to use their social networks mainly passively, since they spend most of the time just checking other people’s posts and looking for information.

Most participants are not ok with giving away their personal information in exchange for a service but do it anyway, since they have accounts for multiple services. This result is consistent with what was found by other studies mentioned in the literature review.

The control of the visibility for the information shared on social networks is of the outmost importance, since almost all participants agree on it. However, only Facebook users feel confident about knowing the public that can see their posts. This is probably due to the amount of privacy settings that the social network provides to its users. In fact, Twitter and Pinterest have a more public strategy. On top of that, since Facebook is the most used service, it is possible that the participants are more at ease with its privacy controls and therefore feel more confident.

This hypothesis is confirmed by the fact that Facebook is the social network where more than three quarters of the participants take their time to make sure that the information they publish is only directed to the intended public. It is interesting to see that a good portion of Twitter users do the same, since there is no direct way to do this on that social network. In fact, most of the tweets are generally public and there is no straightforward way to restrict their audience. The uncertainty about the remaining social networks is consistent with the hypothesis that the users are less at ease with these social networks and don't know their way around them as well as in Facebook.

In the literature review, it was pointed out that the privacy settings are often seen as something static, that people set once and never touch again. This is not entirely the case for Facebook users, since nearly half of them reported having checked them a month before the study. For the other social networks however, users only looked at the privacy settings when creating their account or haven't checked them at all, leaving therefore the default privacy settings provided by the respective social networks. In part, this could be due to the fact that some social networks like Pinterest contain less personal information by nature, therefore making their users more at ease with the management of their privacy. In connection to this, it can be seen that most Facebook users don't trust the default privacy settings suggested by the social network and that could be one of the causes of the more frequent privacy management. The only social network that is trusted by a good portion of its users is LinkedIn. This is probably because, being a professional social network, the information it contains is less private and is posted with the goal of being seen by potential employers and professional contacts.

Privacy policies remain a document that very few people read before accepting. Surprisingly, a third of Facebook users claims to have read it, while on the rest of the social networks the number is extremely low.

Facebook is the social network considered the most dangerous in relation to the possibility of information misuse. In fact, most of its users are concerned about this possibility. That could be because of the kind of personal information that is shared on that social network, since the others could be considered less sensitive.

The literature review has highlighted some difficulties in the management of the privacy settings. This trend is confirmed by the results of this survey, mostly on Facebook. In fact, although three quarters of its users consider the privacy settings easy to find, only less than

50% of the surveyed Facebook users understand what every privacy setting does, and almost half of the participants feel overwhelmed by the quantity of privacy settings to manage.

On the other social networks, users seem to be unsure about how they feel about the privacy settings. This, as stated before, could be partly due to the less frequent use of those services and the consequent limited knowledge about them.

The observed results show that the users that took part to the survey were not very informed about the default settings of the different social networks they have an account for, since they only got half of the default settings right on average, and they seem to think that the various social networks would prefer more private settings by default, since the majority of the mistakes were of stricter nature, i.e. the users thought that the default setting would be stricter than it actually was.

This could pose a problem for the users that don't change their default privacy settings, since the default settings are much more revealing than what they realize.

4.5 Survey limitations

The research had some limitations, due to factors that were not accounted for before its development. In fact, it has to be noted that many of the questions asked to the participants could be subjectively interpreted. It would have been interesting to find a way to test if their subjective opinion corresponded to what they actually did, for example when they claim to know exactly who can see the information they share, similarly to what has been done on Friend Inspector [14].

Social networks like Facebook offer the possibility of instant chat to communicate with other users. This aspect of the platforms, often used as a separated service and mostly involving only a defined set of participants at a time, were not considered in this study.

5

Developing and testing a prototype

The previous chapters analyzed the current research about privacy management on social networks, observed the privacy policies and settings of the considered five services and asked the users about their behavior and concerns about their privacy on these online platforms.

Using the collected results, it is now possible to define the main functionalities for the application prototype to be developed and tested and proceed with the implementation.

5.1 Requirements

The results of the previous chapter indicated a general lack of confidence and information about privacy settings and a general concern about the possible misuse of the information shared on the social networks.

Specifically, users state that they are not sure about the function of the different privacy settings at their disposal. For this reason, the application should provide them with a list of all possible privacy settings and explain what every setting does. To further help the user in deciding how to set the different privacy settings, the tool should give a suggested value and illustrate what could happen if the settings is set to a value that is too open and therefore makes the information it controls too broadly available.

The default settings section of the survey showed how many users don't know what default values are assigned to the privacy settings and often underestimate their default visibility. That's why it is useful to also indicate the default value of every privacy setting, so that a user browsing the application can realize how open the default settings can be and be motivated to check and change their personal privacy settings.

According to the survey, only a very small set of users has read the privacy policy for any of the social networks they have an account for. To help overcome this problem, a summary of the main points treated in the privacy policies, especially the information that is collected and the way that it can be treated and used by the social networks, should be shown to the user. If needed, the user should be able to click on an element and get a more detailed explanation about the specific item.

In the "trust" section of the survey, users asserted their concerns that the information they publish on the social networks could be misused. This means that the application should help

the user check how visible their social media profile is and identify the elements that are publicly available, so that they can consequently remove or hide them if considered necessary.

According to the results of the survey, the users that participated had on average an account for two to three social networks. For this reason, the application should offer its functionalities for more than one social network and, if necessary, allow to compare the values of different services.

Since most users state that they mostly use the desktop web version of the social networks to manage their privacy settings, the application should be developed with this type of interaction in mind.

5.2 Technical specifications

After some thought and since it will only be tested once, the prototype should be medium to high fidelity, instead of just being a non-working low-level prototype. For this reason, it appears appropriate to develop it as a basic web application, so that users can access it from the internet and interact like they normally would. On top of that, past experience from other projects realized during the master lessons, has shown that using a prototyping application without any experience can be expensive or difficult and thus complicate the entire process.

The web application is based on the MVC paradigm, using Ruby on rails as the development framework and HTML5 with Bootstrap for the presentation. To build the view of the application, some elements have been taken and adapted from bootsnipp.com [37].

Every interface is developed as a separate application, derived from the first one developed. On top of that, a test wizard was developed as a fourth application, to allow the remote testing of the prototype and guide the users through the experience.

For the time of the test, all applications are run from a Raspberry Pi 3 at home to avoid hosting fees and are accessible through the internet at the following links:

Test wizard:	http://engid87.asuscomm.com:4500
Interface 1:	http://engid87.asuscomm.com:3100
Interface 2:	http://engid87.asuscomm.com:3200
Interface 3:	http://engid87.asuscomm.com:3300

Table 5 : Links to the four web applications used for the test

Initially the prototype should have had actual information from a person's social network page. After some thought, it's been decided to work with fictional data to make the testers more at ease and to make sure that the test would happen on the same exact conditions and to facilitate the recruiting of people. In fact, when asked to participate to the test, multiple people expressed some concern about giving access to their personal data to someone they didn't know.

Moreover, many people only have accounts for Facebook and another social network, so they wouldn't have an account for the rest and wouldn't therefore be able to test the entire prototype.

Of course, this decision can also have some disadvantages. The most notable one is the fact that, since the information shown is not personal to the user, they feel less concerned about it and therefore the effect of finding out that something is too visible is reduced compared to using real information from their social networks accounts.

5.3 Interfaces overview

A total of three different interfaces have been developed, all of them offering virtually the same functionalities but presenting them in different ways.

In fact, all of them present the possibility to choose between 5 different social networks, contain a list of the available privacy settings for each of the five services with information about what they do, what could happen if they are set too openly and the current, recommended and default values, a section about the social network's privacy policy and one showing the public information visible from the specific profiles as well as an assessment of their profile openness.

All data is hard coded in a database, thus no personal information about the testing user is required or requested.

The complete collection of screenshots of the different interfaces can be found in appendix F.

5.3.1 Interface 1 - Tabs

The main concept of the first interface is dividing the different sections (privacy settings, privacy policy, public information) using 3 different tabs. On the left side of the screen, the user can switch from a social network to another. On small screens, the sidebar collapses automatically, showing only the social networks logos and expands when hovered with the cursor. When first opening the application, the user sees a scrollable list of Facebook's privacy settings. Clicking on a specific setting shows the following fields:

What is it for: explains the purpose of the privacy setting.

What could happen: shows some possible issues that could arise if the setting is set too public.

Current value: shows the actual value selected for the specific setting (fake data, hardcoded).

Recommended value: shows the recommended value for the specific setting.

Default value: shows the default value for the specific setting.

Moving to the privacy tab, the user is presented with 3 panels called respectively "what information can they collect", "what can they do with it" and "who can they share it with". Every panel contains a clickable list of things. When clicked, details appear in a popover.

The third tab gives the user a quick assessment of how private/public their profile is, represented by a percentage number and a progress bar as well as an overview of the public information visible on their profile, divided into “public information”, “public pictures” and “public posts”.

The following figure illustrates the first interface appearance.

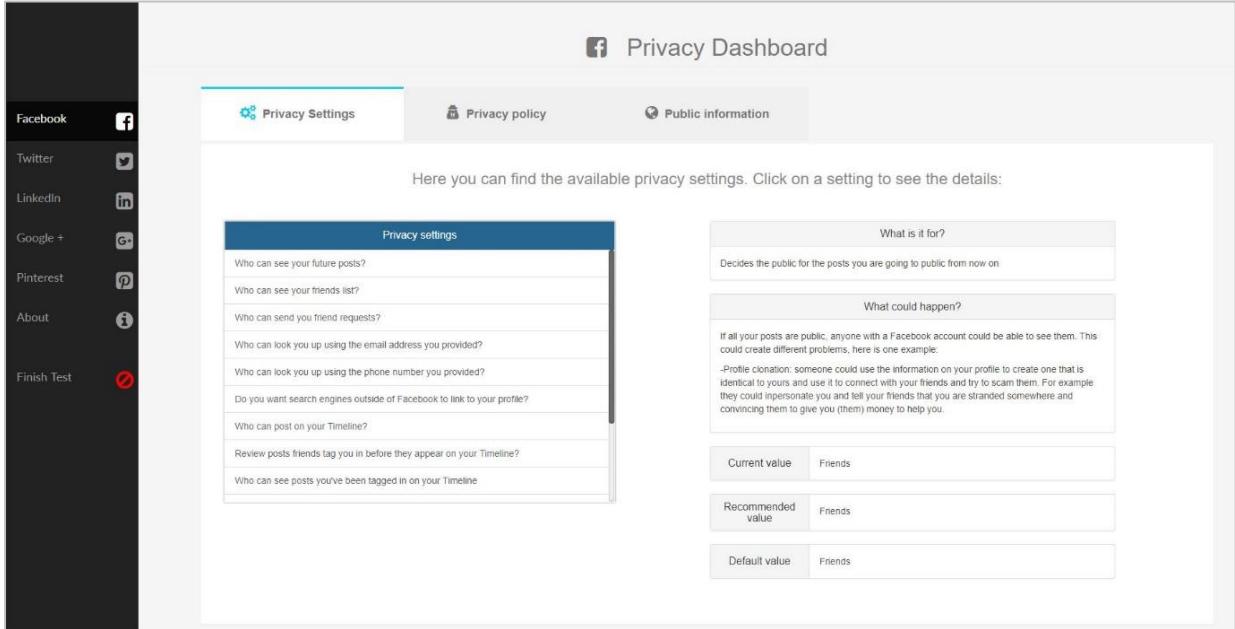


Figure 10 : Screenshot of the first interface

5.3.2 Interface 2 – Tiles

The second interface is similar to the first in the sense that the sidebar on the left is still present and gives the users the possibility to switch from one social network to the other in the same exact way.

Instead of having different sections like in the tabbed interfaces, this one presents the user with 3 square tiles, showing a small preview of the content they contain. The first is about the privacy settings, the second about the privacy policy and the third about the public information. On the bottom right corner of every tile there is a button to expand it and show the full information.

When clicked, the users see the same three panels that they could find on the first interface.

The main difference is in the fact that the user can preview some data from each tile, thus potentially speeding up the search for the information they are looking for.

The following figure illustrates the second interface appearance.

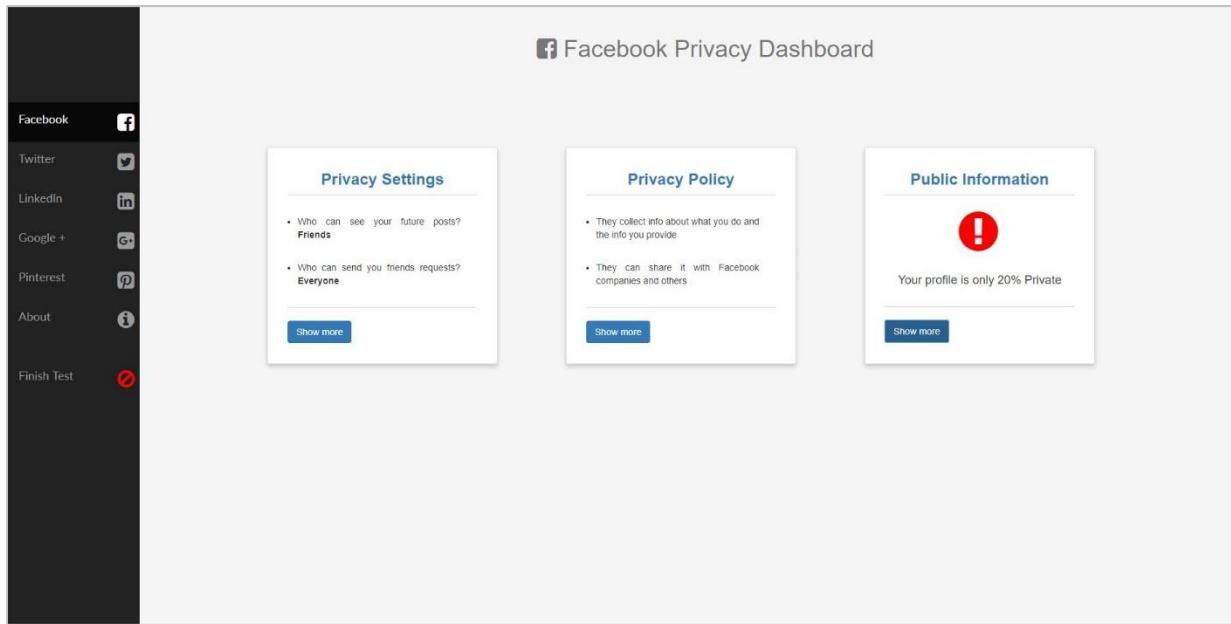


Figure 11 : Screenshot of the second interface

5.3.3 Interface 3 – Columns

The third interface changes the disposition of the different elements. Instead of using the left sidebar to select the social network, the user must use it to switch from the three different sections, Privacy settings, Privacy policy and Public information. Three dropdown menus are present on every page and give the user the possibility to select up to three social networks. This way, the user can easily compare the data between different social networks, without having to go from a page to the other.

On the privacy setting's page, after selecting the preferred social network(s), the user is presented with a list of privacy settings and their current value. When clicking on a single setting, the same information as in the other interfaces is shown in a popover, in text form.

In the privacy policy page, after selecting the social network, an accordion is shown, with 3 expandable sections “what information can they collect”, “what can they do with it” and “who can they share it with”.

The public information page follows the same structure, but presents the privacy assessment as well as a collection of publicly visible profile information, pictures and posts. The following picture shows a screenshot of the third interface.

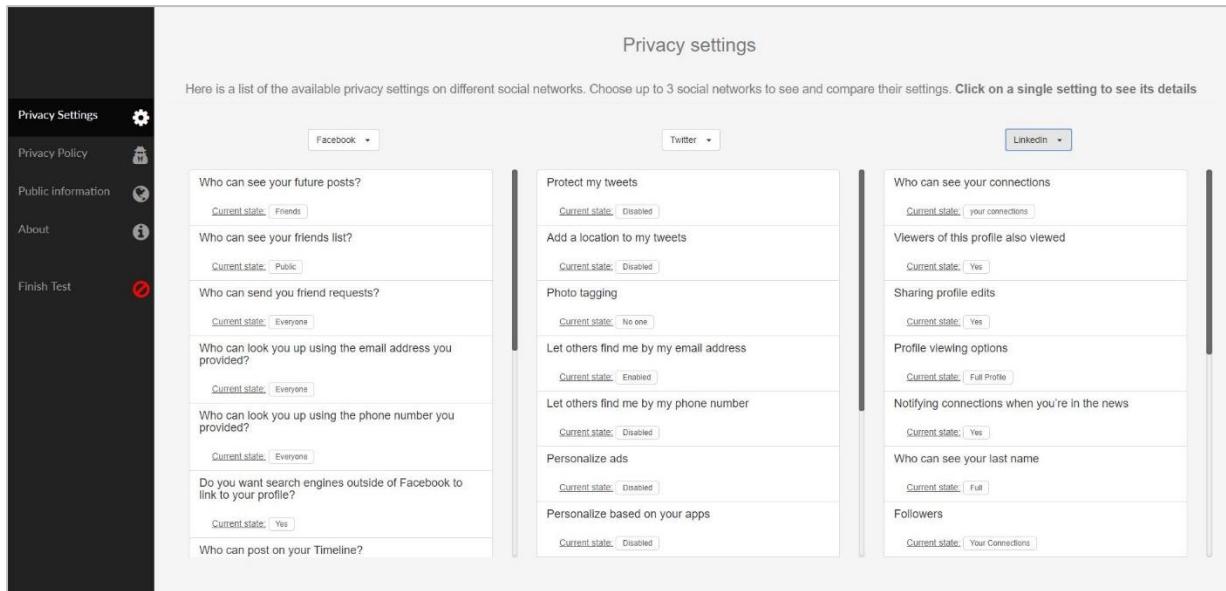


Figure 12 : Screenshot of the third interface

5.4 Test

The goal of the test is to assess following aspects of the privacy dashboard and raise the user awareness about the privacy on social networks:

- Usability
- Usefulness
- Gather information / input about possible improvements

Before the start of the test, the following hypotheses were formulated:

- H1: “Tiles” interface is the quickest to use, thus generates the lowest completion times. Since part of the information is already shown in the form of small previews, it will be quicker for the user to retrieve it, without having to look in the main window.
- H2: “Columns” interface is the easiest and quickest for comparing social networks. Since this interface allows the user to have up to three social networks side by side, less actions are required to compare information from different social networks and therefore this interface makes this task easier and quicker.
- H3: “Tiles” interface is the most liked by the users. this interface is the one that requires less interaction from the user and therefore is expected to be the one preferred by the participants.
- H4: Users find the tool useful.
- H5: Users learn something by using the tool.
- H6: If available, users would use it.

5.4.1 Method

To test the usability and usefulness of the three developed interfaces, a usability test has been performed on a total of 18 subjects. Due to the lack of participants on site, the test has been performed remotely to increase the chances of finding enough subjects.

According to Andreasen and al. [38], a synchronous remote usability test can provide virtually the same results a regular lab-based think aloud experiment and therefore this shouldn't cause any problem.

The test consisted in a controlled experiment, where the participants had to perform a set of predefined tasks using the three different interfaces and describe the experience by answering some follow up questions.

A test wizard was developed to guide the participants during the experience. The full series of screenshots can be found in appendix D. After accessing the landing page, the participant had to read a brief description of the test and its purpose, as well as a short privacy policy describing what information would have been recorded during the test.

The following screen asked a set of initial questions, to find out some demographic data about the participant and their use of social networks:

- Gender
- Age
- How concerned do you consider yourself about your privacy on social networks, on a scale from 1 (I don't care) to 5 (I care a lot)?

The user had the possibility to rate on a scale going from 1 to 5.

- In my opinion, a social network's privacy policy defines:

The user had the choice between “What information the other social network users can see about me”, “What information the social network can collect about me and what they do with it” and “I don't know”.

- How often do you use/visit the following social networks?

The user could answer on a six-point scale composed by “Hourly”, “Daily”, “Weekly”, “less often” and “I don't have an account”.

- How often do you POST something on the following social networks?

The user could answer using the same scale as for the previous question.

- When was the last time you checked your privacy settings?

The user could answer using a 5-point scale going from “last week” to “last month”, “last year”, “when creating the account” and “never”.

Once this task completed, the subjects had to download a small portable program, TeamViewer QS, and transmit the displayed login data, necessary to access their computer remotely and observe their actions on the screen. The users had the possibility to choose the amount of data

recorded between “screen only”, “screen and microphone” and “screen, microphone and webcam”, like specified on the first description in the landing page.

Once everything set, the user could go to the following screen and watch a short video tutorial explaining what to do.

This is the point where the test actually began. The participants were presented with a button to open one of the interfaces on a new tab in their browser and a list of tasks to accomplish, like shown in the following figure.

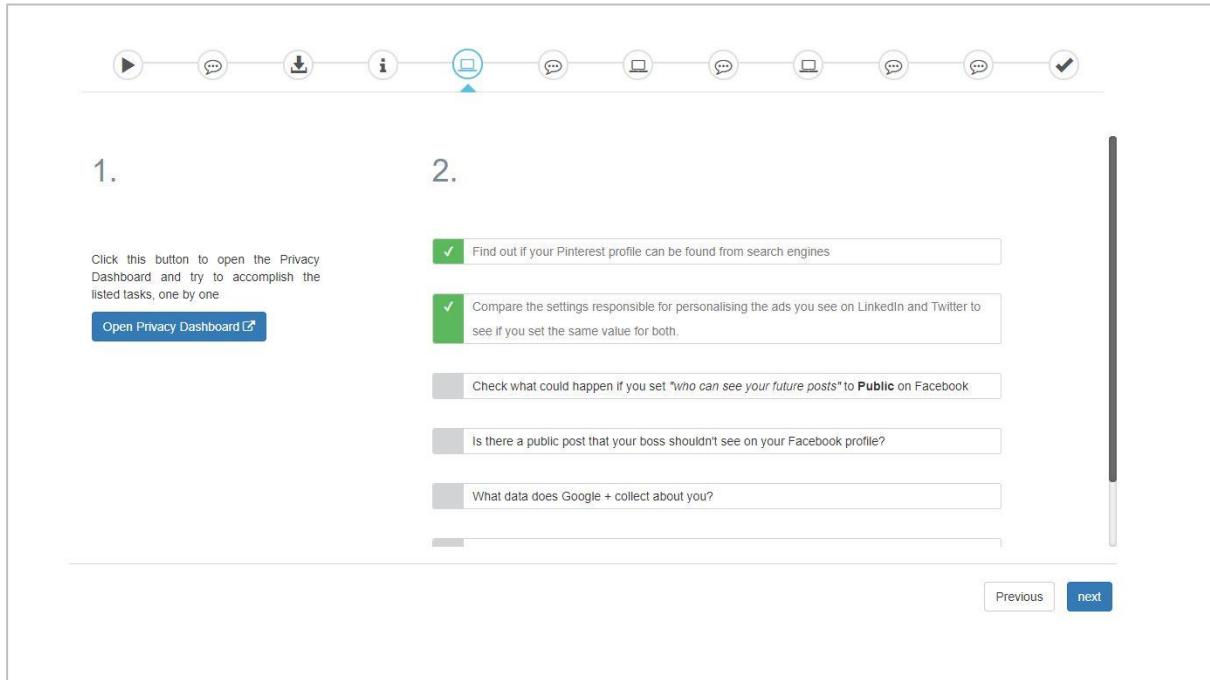


Figure 13: Screenshot of the list of *tasks* to accomplish on the test wizard

The users had to carefully read the instruction, switch to the interface tab, try to accomplish it and, once they thought to have completed the task, go back to the instruction tab and mark the task complete. They did the same for all instructions one by one until the end of the list.

The tasks asked the user to find specific information using the tool, which could be of four types:

- Information about a privacy setting.
- Information about the collection or usage of personal information by the social network, specified in the privacy policy.
- Look for a specific element that was publicly visible.
- Comparison between similar settings on different social networks.

The complete list of all the tasks can be found in appendix E.

After completing all the tasks, participants were asked to fill in a short questionnaire, asking them how easy it was to use the interface they had just tested and how easy it was to compare

the information between different social networks. If needed, a field to write additional commentary was provided.

The same procedure was repeated for all three interfaces and was concluded by a final questionnaire, where participants were asked what interface they liked the most and a series of questions about the usefulness of the tool in general.

In order to counterbalance the more than likely learning effect, the order of the three tested interfaces was rotated every time, every combination being tested by at least three people and every interface being used in every position six times.

A set of quantitative and qualitative data were gathered during the test and, when possible, analyzed using IBM SPSS 24:

- Steps accomplished by the users: observe how users try to complete the task, what sections they go to.
- Specific UI problems: according to the previous observation, find out what the major problems are.
- Something new learned by the user: according to the answers given in the final questionnaire.
- User suggestions, improvements: comments given by the users in the questionnaires.
- Time to finish the set of tasks: every task was timed from the moment the user switched to the dashboard tab to the moment they marked it finished and the single timings were added to get a set's total time.
- Number of successfully completed tasks: the tasks performed by the user were evaluated with 3 possible values: “0” to indicate that the user didn't find the information they were looking for or found the wrong answer, “0.5” if the user went to the right section but didn't find the specific information or if only part of the information was found and “1” if they found the information they were looking for. The values were then summed to get the number of successfully completed tasks on a defined set.
- Ease of use: indicated by the user in each post-test questionnaire.
- Usefulness: indicated by the user in the final questionnaire.
- User preference: user choice on the final questionnaire.

5.4.2 Results

Participants

A total of 18 participants tested the different interfaces. The majority of the testers were males (66.7%) aged between 21 and 30 years old (77.8%) who have an account for 3 social networks on average (2.55), one of which is always Facebook (100%). They use Facebook hourly (38.9%) or daily (44.4%) and post something weekly (33.3%), monthly (33.3%) or less often

(27.8%). The other social networks are mainly used less often, independently if it is for watching or posting.

The users indicated their concern for their privacy to be a 4 out of 5 on average and the majority (72.2%) indicated that a privacy policy defines what information the social network can collect about the user and what they can do with it, while the remaining 27.8% choose the other answer. Finally, the participants said to have last checked their privacy settings mainly a month before the test (38.9%) or a year before (38.9%) on Facebook and when creating the account or never on the other social networks.

Quantitative data

After the tests, the results were analyzed to try to understand if one of the three possible interfaces was faster to use or led to less errors.

Every task was timed and the total time for the three interfaces was compared to look for significant differences. The following table shows the mean and standard deviation of the three measurements:

	Mean	Std. Deviation
Time to finish: tabs	05:49.94	03:09.18
Time to finish: tiles	06:45.78	03:23.38
Time to finish: columns	06:16.89	04:52.98

Table 6: Average time to finish an interface test

By looking exclusively at the mean of the time, there doesn't seem to be a significant difference between the three interfaces. To confirm this result, a repeated measures ANOVA was performed without finding any statistically significant difference: $F(2, 34) = .902, p = .415, \eta_p^2 = .050$.

In an analogous way, the percentage of successfully completed tasks was also analyzed, as it can be seen in the table below:

	Mean	Std. Deviation
Percentage of successfully completed tasks: Tabs	.7639	.2026
Percentage of successfully completed tasks: Tiles	.7176	.2142
Percentage of successfully completed tasks: Columns	.7778	.2081

Table 7: Average percentage of successfully completed tasks

Once again, these results don't seem to indicate a significant difference between the amount of successfully completed tasks between the three interfaces. Further analysis confirms the lack of a statistically significant difference: $F(2, 34) = .728, p = .490, \eta_p^2 = .041$.

Additional analyses have been performed to try to understand if one of the three interfaces led to significantly different results in one of the task types, compared to the other two interfaces.

A significant difference has been found in the completion time of the tasks involving the retrieval of information from a social network's privacy policy ($F(2, 34) = 4.072$, $p = .026$, $\eta_p^2 = .193$) and the comparison of privacy settings between different social networks ($F(2, 34) = 7.921$, $p = .001$, $\eta_p^2 = .318$).

In fact, the "Tabs" interface resulted significantly quicker to use than the "Tiles" one in tasks concerning information in the social network privacy policy and quicker than the "Columns" one, even though the latter was not statistically significant. Comparing privacy settings between two different social networks was significantly slower on interface "Tabs", compared to the other two variations of the interface, as it can be seen in the following tables showing the mean difference between interfaces. Values marked with * are significant at the .05 level.

		Mean Difference (I-J, in seconds)		
(I)	(J)		Std. Error	Sig.
Tabs	Tiles	-41.778*	10.087	.002
	Columns	-22.944	14.965	.431
Tiles	Tabs	41.778*	10.087	.002
	Columns	18.833	17.870	.920
Columns	Tabs	22.944	14.965	.431
	Tiles	-18.833	17.870	.920

Table 8: Pairwise comparisons - Time to complete a "privacy policy" task

		Mean Difference (I-J, in seconds)		
(I)	(J)		Std. Error	Sig.
Tabs	Tiles	49.556*	14.582	.010
	Columns	32.167*	11.907	.045
Tiles	Tabs	-49.556*	14.582	.010
	Columns	-17.389	11.156	.412
Columns	Tabs	-32.167*	11.907	.045
	Tiles	17.389	11.156	.412

Table 9: Pairwise comparisons - Time to complete a "comparison" task

On the other hand, no significant difference between the percentage of successfully completed tasks of a certain type have been observed among the three interfaces.

After every interface test, the user was asked to say how easy they found using the interface and how easy it was to use it to compare information between social networks using a five-point Likert scale.

The "Tabs" interface was rated average to use by the majority of the users that tested it (66.7%), while the "Tiles" interface was rated average by 50% of the testers and easy to use by 33.3%

of them. The “Columns” interface was considered average by 38.9% of the testers and easy to very easy by most of the remaining users (22.2% each). The complete evaluations can be seen in the figure below.

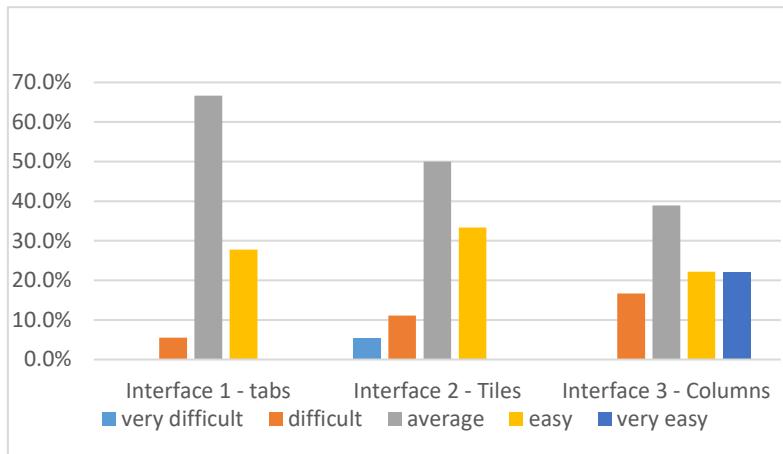


Figure 14: Subjective ease of use of every interface

The mean and standard deviation of the three interfaces’ evaluation (1= very difficult, 5= very easy) were calculated, giving the following results:

	Mean	Std. Deviation
Interface 3- Columns	3.5000	1.04319
Interface 2 - Tiles	3.1111	.83235
Interface 1- tabs	3.2222	.54832

Table 10: Average user evaluation per interface

By looking at the average evaluation given by the users, it seems like the “Columns” interface is slightly easier to use compared to the other two interfaces.

Just like before, a repeated measure ANOVA has been performed to check for statistically significant differences between the three interfaces and no significant difference was found: $F(2, 34) = 1.277, p = .292, \eta^2_p = .070$.

27,8% of the users defined the “Columns” interface to be very easy and 33.3% easy for comparing information between social networks. The “Tiles” interface had 44.4% of the users defining it easy for comparing information and 33,3% average while on the “Tabs” interface the comparison was rated easy by 33.3% of the users and average by 44.4% of them, as it can be seen in the figure below:

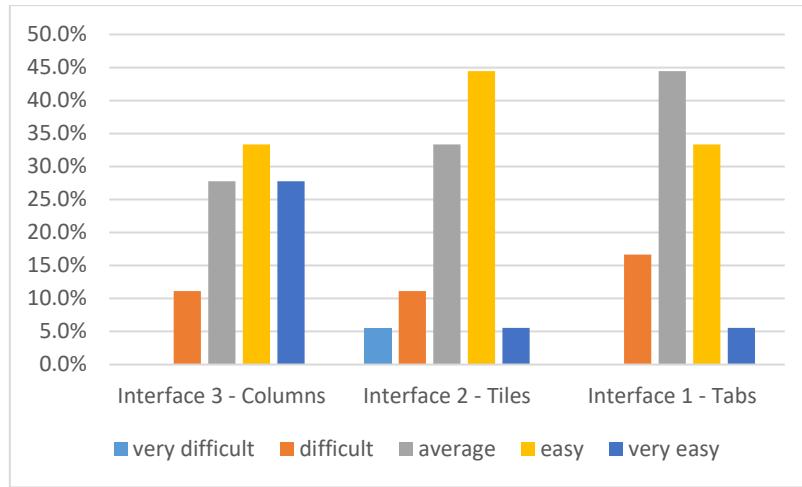


Figure 15: Ease of comparison between social networks per interface

Once again, the average evaluation was calculated and generated the following results:

	Mean	Std. Deviation
Interface 3 - Columns	3.7778	1.00326
Interface 2 - Tiles	3.3333	.97014
Interface 1 - Tabs	3.2778	.82644

Table 11: Average evaluation for comparing information between social networks

At first sight it would appear like the “Columns” interface could be considered slightly easier to use by the users who participated to the test but just like for the previous analyses, no statistically significant difference was found: $F(2, 34) = 2.657, p = .085, \eta_p^2 = .135$.

When asked for the interface they liked the most, the participants showed a slight preference for the “Tabs” interface. In fact, 38.9% of them indicated this preference, followed by the “Columns” interface with 33.3% of the votes and finally by the “Tiles” interface, that scored a 27.8% preference.

The final questionnaire asked the users a series of questions regarding the utility and effects of the prototype in general.

The privacy dashboard was found useful by most users (38.9% agree, 55.6% strongly agree) who think that it provides useful information about privacy on social networks (mean evaluation 4.5 out of 5, std. deviation .618). A similar result was obtained for the privacy assessment (33.3% agree, 50% strongly agree, mean evaluation 4.33 out of 5, std. deviation .766), the box that indicated graphically how private a user’s profile was. Using the tool made most of the participants think more about their privacy on social networks (50% agree, 27.8% strongly agree, mean evaluation 4 out of 5, std. deviation .840) and more than half of the testers learned something new by testing the privacy dashboard (44.4% agree, 22.2% strongly agree, mean evaluation 3.77 out of 5, std. deviation .94).

Finally, most users affirmed that, if the privacy dashboard was a final and publicly available tool, they would probably use it (55.6 % agree, 27.8% strongly agree, mean evaluation 4 out of 5, std. deviation .97).

Qualitative data

During the multiple tests, a series of observations about the general usability of the prototype could be made and some feedback from the users could be collected. Here are the main findings, divided by interface.

Interface 1 – Tabs

One of the main observed problems of this interface is the lack of visibility of the three tabs on the top that allow the users to switch between the sections “Privacy Settings”, “Privacy policy” and “Public information”. In fact, multiple users only saw the first section and had therefore some problems when they had to accomplish a task that asked them to retrieve some information from the privacy policy or to look for public information.

The menu on the left, used to switch from a social network to the other, seems not to be very visible as well, since multiple users needed some time to realize how to switch from one social network to the other, especially if it was the first of the three interfaces they tested.

When looking for a picture on the public section, users would close the appearing modal window every time, not noticing the two arrows on the sides to scroll from a picture to the next, respectively previous.

Interface 2 – Tiles

The “Tiles” interface, with the 3 tiles showing the main points of every corresponding section, should have been the easiest and quickest to use. In reality, virtually all the users completely ignored the information that was shown in the tiles, even if it corresponded to what they were looking for. In fact, they always clicked on the “Show more” button to see the complete list of information and wandered between all elements before finding the right one.

Like for the “Tabs” interface, the menu on the left wasn’t noticeable at first, especially if it was the first interface they used.

One bug was found and annoyed most of the users: when clicking on a photo in the “public information section” and opening the corresponding modal with the enlarged picture, it wasn’t possible to close the modal without returning to the main screen. This is due to the way modals work in bootstrap and a workaround needs to be found to prevent this problem.

Once the detailed view was open, the navigation worked just like on the “Tabs” interface and therefore the encountered problems were the same.

Interface 3 – Columns

The third interface was centered on comparing information between different social networks. Users immediately understood how to find the needed social network. Strangely enough, some users didn’t use the possibility to select multiple social networks on the same page when

comparing information but used only one selector to look for both social networks, one at a time.

Like in the other two interfaces, the menu on the left was not seen by the majority of users, even if this interface wasn't the first they had tested. The problem was greatly increased on narrow screens, where the sidebar was collapsed and only showed the icons relative to the various menu items, since the used icons don't seem to be intuitive at all.

Since the menu contained the links to the "privacy policy" and "public information" sections, this made it difficult for many users to find the corresponding information.

One annoyance was found by multiple users: when switching from one section to the other, the user had to re-select the social networks they had selected before. It would be much easier and quicker if the tool could remember what social networks were selected and open them again once the section was switched.

General observations and feedback

In general, the users seemed to have some difficulty knowing where to look to find the requested information. In fact, they tended to look for everything in the settings instead of going directly to the "privacy policy" or "public information" sections. Even after noticing the various sections, most users tended to first look between the privacy settings and then checked every single information on the page until they found what they were looking for.

Like already noted before, the menu on the left was difficult to see for the majority of the users, especially on narrow screens where it was collapsed and only the icons were shown.

Some users suggested that it would be useful to have a starting page where only the information that needed attention, like settings that don't correspond to the recommended value or public sensitive information, is shown, so that they don't have to check every item to see it.

Another suggestion was to add a search module, to make it faster to look for a specific information.

5.4.3 Discussion and future development

Before the start of the test, six hypotheses were formulated about the expected results of the tests, but not all of them have been confirmed by the actual discovered results:

- H1: Tiles interface would be the quickest to use.

This hypothesis could not be confirmed by the test results. In fact, no statistically significant difference has been found between the total time needed to complete the set of tasks assigned to every interface. The analysis of the specific task types has even shown how the "Tabs" interface was significantly quicker to use in tasks concerning information from the social network's privacy policy.

- H2: Tiles interface would be the favorite by the users.

Despite the slight preference for the “Columns” interface that both mean evaluations seemed to give at first glance, a slight majority of users choose the “Tabs” interface as their favorite, while the “Tiles” interface was the least voted of the lot, meaning that this hypothesis cannot be confirmed by the results found. Since the quantitative results don’t show any significant difference between the interfaces, it is probable that this preference is merely visual and therefore due to the graphical presentation instead of the interface structure.

- H3: Columns would be the easiest and quicker to compare information between social networks.

Quantitative results show that the comparison tasks were significantly slower on the “Tabs” interface, compared to the other two. There is however no statistically significant evidence that the “Columns” interface is quicker for comparing information between different social networks.

When asked about their preference, the testers expressed a slight preference for this interface but, since the difference is not statistically significant, it is not sufficient to confirm this third hypothesis.

- H4, H5, H6: Users would find the tool useful, learn something new by using it and use the tool if finished and publicly available.

According to the evaluations given by the users at the end of the test, the privacy dashboard seems to be a useful concept that gave the participants useful information about the privacy on social networks and helped them learn something new about privacy on these services.

In fact, most of the participants agreed that they would use it if available which, on one side confirms the need for help in the management of the privacy on social networks and, on the other, makes the possibility of ulterior improvement and the eventuality of public diffusion of the tool a valid possibility.

In general, the three interfaces didn’t provide significantly different results regarding the time needed to finish a set of tasks or the number of successfully completed tasks. A possible explanation for this could be the fact that the underlying functionality and provided information was the same for the three interfaces. In fact, the steps that the users had to accomplish were similar, independently of the tested interface and only the graphical presentation was different. The average evaluation for all three interfaces was situated between 3 (average) and 4 (easy), but the percentage of successfully completed tasks was relatively high for all interfaces. This indicates that some work and refining is needed but the main concept and structure is good.

Even though most people chose the right answer when asked about the contents of a privacy policy, the idea of what it contains doesn’t seem to be clear since most users, when asked to find out what information the social network can collect about them or who they can share it with, just wandered around without going straight for this section. This result could be considered consistent with the findings of the survey conducted in chapter 4, since most users admitted never reading any of the social networks’ privacy policies.

Future developments

According to the test results and to the feedback received from the users that tested the tool, the following improvements could help improve the prototype:

- Landing page with notifications

More than one user suggested that a landing page that shows only the settings and information that requires attention from the user would allow to quickly correct small errors and give an overview of the general state of the accounts.

- Better visibility for menu

From the observed tests, it is clear that the menu on the left is not visible enough. This could be due to its colors or lack thereof, since it is completely black and it's probably seen as part of the tool at first glance. Adding a bit more color, for example to differentiate the various menu items, could improve the visibility of the menu. To make the navigation faster, the menu could include both the various social networks and the different sections, for example in a sub-menu. Since the icons used for the “privacy settings”, “privacy policy” and “public information” don't seem to be intuitive and don't seem to mean anything to the user when the menu is collapsed, integrating the two menus together could help solve this problem.

- Small walkthrough at the beginning to show the different sections

Users that tested the prototype didn't seem to understand clearly the use of the three different sections included with every social network. To help this problem, a short walkthrough in the form of small callouts could be shown on first use to show the user where they can find the information.

- Search module

Looking for a specific information can be tedious and time consuming on the current state of the tool. A search module could help make this much faster and make the navigation easier. The downside of this approach would be that by finding the information directly, users would skip the rest of the tool and therefore the general awareness improvement would be reduced.

5.4.4 Limitations of the prototype and the test

It is always difficult to foresee every single variable in this kind of test and therefore there are some aspects that could have been improved.

Regarding the development of the prototype, it would have probably been possible to create a single application instead of four. That way, it would have been easier to maintain, since there would have been a single shared database.

Even if most of the possible bias sources have been accounted for, there were still some aspects that were not taken into consideration before the test. It's only been realized afterwards that, even though only participants with a good English level were recruited, the results of the test could be influenced by the language of the interface, since none of the participants were of

English mother tongue. An effective way to avoid this problem would have been to translate the entire prototype and test in French and Italian.

In addition to that, the order of the tested interfaces was rotated to counterbalance a very probable learning effect, but the tasks weren't. In fact, every list of tasks was linked to a particular interface and the single tasks were always performed in the same order.

Finally, the tasks that asked to find a specific public picture or post could probably have been written in a clearer way, since virtually all the participants had some trouble performing them.

6

Conclusion

The goal of this master thesis was to build a prototype for a “Privacy Dashboard”, a tool to allow social networks users to have a quick overview of their privacy settings and other privacy related information.

The first chapter analyzed the existing literature to find out if there was the need for such a tool. This literature research has showed that the privacy on social network is an aspect that is not very easy to manage. A considerable amount of information is shared continuously and, if not correctly managed, could lead to multiple problems.

To be able to correctly manage their privacy on social networks, users need to be aware of the problem and its possible consequences as well as the tools at their disposal to do it.

According to the analyzed papers, many users still lack this kind of awareness, since they don't take the necessary measures to protect themselves. On top of that, users that use the privacy settings to manage their privacy often find it difficult and tedious, which can lead them to make mistakes.

The following chapter observed five distinct social networks to see and better understand some aspects related to the privacy: their privacy policy, their default settings and the usability of their privacy management pages. The analyzed privacy policies turned out to be similar across the social networks: the kind of information that is collected by every social network tends to be the same as what the others do. All documents are relatively easy to read but require a minimal understanding of the subject to fully understand what they mean.

In the third chapter a survey was developed and run with social network users to find out if the problems highlighted in the literature review were still actual and applied to the asked population. The results show that there is still a certain difficulty and a feeling of insecurity surrounding the management of the privacy on social networks, partly due to the lack of information and understanding on the side of the users and to a complicated and time-consuming management system offered by the social networks.

The last chapter was dedicated to the conception, development and testing of a prototype for an application to help the users solve or at least reduce these problems: the Privacy Dashboard. The tool allows the users to check the privacy settings available on the social networks they are logged in to, better understand what every one of these option does and what could happen if they were not set to the desired degree of openness. Furthermore, the user can check the current state of their settings and compare it with a suggested value.

The tool also shows the users a short version of the contents of every social network's privacy policy, allowing them to be informed about the information that those services collect about them and the way their information is used and shared.

A third functionality of the privacy Dashboard allows its users to check what information from their profiles is publicly visible to anyone with a social network account, so that they can act to correct it if necessary.

To find the right aspect and functionality for the tool, three different interfaces have been developed and tested with 18 users. The results indicated that none of the developed interfaces was significantly better than the others and that the overall usability was average to good. This means that there is still work to do, but the main idea is solid and liked by the users. In fact, most of them, after testing the prototype, expressed interest for such a tool and said to have learned something new that made them think more about their privacy on social networks. Knowing how a user's information is collected and used on this kind of services is the first step towards effectively managing it to take control over someone's data and this work represents a step forward in that direction.

7

References

-
- [1] “Number of social media users worldwide 2010-2021 | Statista,” 2017. [Online]. Available: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>. [Accessed: 19-Nov-2017].
 - [2] N. Guy-Hermann Ngambeket, “Social Networks and Privacy - Threats and Protection,” *ISACA J.*, vol. 5, pp. 18–19, 2012.
 - [3] S. Guo and K. Chen, “Mining privacy settings to find optimal privacy-utility tradeoffs for social network services,” in *Proceedings - 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012*, 2012, pp. 656–665.
 - [4] M. Onuma, A. Kimura, and N. Mukawa, “Exploring social cognition related to privacy settings in SNS usage,” *Proc. - 2013 Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2013*, pp. 1077–1082, 2013.
 - [5] A. Kuczerawy and F. Coudert, “Privacy settings in social networking sites: Is it fair?,” *IFIP Adv. Inf. Commun. Technol.*, vol. 352 AICT, pp. 231–243, 2011.
 - [6] “Facebook - Nutzer in der Schweiz 2017 | Statistik,” 2017. [Online]. Available: <https://de.statista.com/statistik/daten/studie/70221/umfrage/anzahl-der-nutzer-von-facebook-in-der-schweiz/>. [Accessed: 14-Oct-2017].
 - [7] “Want a Google Account? Now You’re Automatically Signed Up for Google+ | TIME.com,” 2012. [Online]. Available: <http://techland.time.com/2012/01/20/want-a-google-account-now-youre-automatically-signed-up-for-google/>. [Accessed: 14-Oct-2017].
 - [8] J. Constine, “Facebook now has 2 billion monthly users... and responsibility | TechCrunch,” *Techcrunch*, 2017. [Online]. Available: <https://techcrunch.com/2017/06/27/facebook-2-billion-users/>. [Accessed: 31-Aug-2017].
 - [9] V. Hiranandani, “Privacy and security in the digital age: contemporary challenges and future directions,” *Int. J. Hum. Rights*, vol. 15, no. 7, pp. 1091–1106, 2017.
 - [10] D. Crawford and V. Chan, “Facebook Reports Second Quarter 2017 Results,” 2017.
 - [11] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, “Analyzing Facebook Privacy Settings: User Expectations vs. Reality,” in *IMC ’11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011, pp. 61–70.
 - [12] M. Kajtazi, B. Johansson, J. Wieslander, and P. Saliaropoulou, “Individual’s privacy management behaviour on the social networking sites (SNS) Examining the actual use

of the privacy settings,” Lund University - School of Economics and Management, 2016.

- [13] M. Madejski, M. Johnson, and S. M. Bellovin, “A Study of Privacy Setting Errors in an Online Social Network,” *2012 IEEE Int. Conf. Pervasive Comput. Commun. Work. PERCOM Work.* 2012, no. March, pp. 340–345, 2006.
- [14] A. Cetto *et al.*, “Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks.”
- [15] F. Stutzman, R. Gross, and A. Acquisti, “Silent Listeners: The Evolution of Privacy and Disclosure on Facebook,” *J. Priv. ...*, no. 2, pp. 7–41, 2012.
- [16] M. Madden, “Privacy management on social media sites,” 2012.
- [17] “ShareMeNot.” [Online]. Available: <http://sharemenot.cs.washington.edu/>. [Accessed: 21-Oct-2017].
- [18] “Privacy Badger | Electronic Frontier Foundation.” [Online]. Available: <https://www.eff.org/privacybadger>. [Accessed: 21-Oct-2017].
- [19] “Facebook Privacy Watcher.” [Online]. Available: <http://www.daniel-puscher.de/fpw/index.php>. [Accessed: 21-Oct-2017].
- [20] “Disconnect for Facebook.” [Online]. Available: <https://addons.mozilla.org/en-US/firefox/addon/facebook-disconnect/>.
- [21] “AVG PrivacyFix.” [Online]. Available: <http://uk.pcmag.com/avg-privacyfix-for-iphone/824/review/avg-privacyfix-for-iphone>. [Accessed: 22-Oct-2017].
- [22] “AVG PrivacyFix replacement? | AVG,” 2016. [Online]. Available: <https://support.avg.com/answers?id=906b0000000cKPqAAM>. [Accessed: 22-Oct-2017].
- [23] “How to Uninstall PrivacyFix | AVG Support.” [Online]. Available: <https://support.avg.com/SupportArticleView?l=en&urlName=How-to-uninstall-Privacyfix&q=Support+for+AVG+PrivacyFix&supportType=home>. [Accessed: 22-Oct-2017].
- [24] “Privacy Check.” [Online]. Available: <http://www.rabidgremlin.com/fbprivacy/>. [Accessed: 22-Oct-2017].
- [25] “McAfee Social Protection Locks Down Your Facebook Photos | PCWorld,” 2012. [Online]. Available: https://www.pcworld.com/article/260286/mcafee_social_protection_locks_down_your_facebook_photos.html. [Accessed: 22-Oct-2017].
- [26] “McAfee Social Protection.” [Online]. Available: http://beta.mcafee.com/betamcafee/mspbeta_lp.aspx?cookieCheck=true.
- [27] “Friend Inspector - Do you know who can see your Facebook profile?” [Online]. Available: <http://www.friend-inspector.org.s3-website-eu-west-1.amazonaws.com/>. [Accessed: 22-Oct-2017].
- [28] “Terms of Service; Didn’t Read.” [Online]. Available: <https://tosdr.org/>. [Accessed: 22-Oct-2017].
- [29] “What is privacy policy? definition and meaning - BusinessDictionary.com.” [Online]. Available: <http://www.businessdictionary.com/definition/privacy-policy.html>. [Accessed: 30-Jul-2017].

- [30] A. M. McDonald and L. F. Cranor, “The Cost of Reading Privacy Policies,” *I/S A J. Law Policy Inf. Soc.*, vol. 4:3, pp. 543–568, 2008.
- [31] Facebook Inc., “Facebook Data Policy.” [Online]. Available: <https://www.facebook.com/policy.php>. [Accessed: 31-Aug-2017].
- [32] T. Inc., “Twitter | Privacy policy.” [Online]. Available: <https://twitter.com/en/privacy>. [Accessed: 31-Aug-2017].
- [33] LinkedIn, “Privacy Policy | LinkedIn.” [Online]. Available: <https://www.linkedin.com/legal/privacy-policy>. [Accessed: 31-Aug-2017].
- [34] Google Inc., “Google - Privacy and terms.” [Online]. Available: <https://www.google.com/policies/privacy/>. [Accessed: 31-Aug-2017].
- [35] P. Inc., “Pinterest | Privacy policy.” [Online]. Available: <https://policy.pinterest.com/en/privacy-policy>. [Accessed: 31-Aug-2017].
- [36] Limesurvey, “LimeSurvey: the online survey tool - open source surveys.” [Online]. Available: <https://www.limesurvey.org/>. [Accessed: 31-Aug-2017].
- [37] “Home of free code snippets for Bootstrap | Bootsnipp.com.” [Online]. Available: <https://bootsnipp.com/>. [Accessed: 05-Nov-2017].
- [38] M. S. Andreasen, H. V. Nielsen, S. O. Schrøder, and J. Stage, “What happened to remote usability testing?,” in *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07*, 2007, p. 1405.

8

Appendices

A

Default privacy settings

Below is a list of the available privacy settings on the analyzed social networks with a brief description of their function and their respective possible and default values.

Facebook

Who can see your future posts?

This setting decides the public for the future posts that the user is going to publish. This value can be set every time something is published.

Possible values: Public, Friends, Friends except..., Specific friends, Only me, Custom.

Default value: Friends.

Who can see your friends list?

This setting decides who on Facebook can see the user's friend list.

Possible values: Public, Friends, Only me, Custom.

Default value: Public.

Who can send you friend requests?

Decides who on Facebook can send the user a request to become their friend and therefore add them to their contacts list.

Possible values: Everyone, Friends of friends.

Default value: Everyone.

Who can look you up using the email address you provided?

Decides who on Facebook can find a user's profile by inputting their email address in the search field.

Possible values: Everyone, Friends of friends, Friends.

Default value: Everyone.

Who can look you up using the phone number you provided?

Decides who on Facebook can find a user's profile by inputting their phone number in the search field.

Possible values: Everyone, Friends of friends, Friends.

Default value: Everyone.

Do you want search engines outside of Facebook to link to your profile?

Decides if the user's profile can be found in the results of search engines like Google.

Possible values: Yes, No .

Default value: Yes.

Who can post on your Timeline?

Decides who on Facebook can publish something on a user's timeline.

Possible values: Friends, only me.

Default value: Friends.

Review posts friends tag you in before they appear on your Timeline?

Decides if the user prefers to manually check every post they are tagged in before it is published on their timeline. This does not control what other people see on their news feed, the tag will still be there, just not on the user's timeline.

Possible values: Enabled, Disabled.

Default value: Disabled.

Who can see posts you've been tagged in on your Timeline

Decides who on Facebook can see posts that someone published on the user's timeline and that the user is tagged in.

Possible values: Everyone, Friends of Friends, Friends, Only me, Custom.

Default value: Friends of friends.

Who can see what others post on your Timeline?

Decides who on Facebook can see the posts that other users have published on the user's timeline.

Possible values: Everyone, Friends of friends, Friends, Only me, Custom.

Default value: Friends.

Review tags people add to your own posts before the tags appear on Facebook?

Decides if the user wants to manually approve every tag that their friends put on the user's published content before they are visible.

Possible values: Enabled, Disabled.

Default value: Disabled.

When you're tagged in a post, who do you want to add to the audience if they aren't already in it?

When a user is tagged on someone else's post, the user can decide who can see that post even if they are not friends with the person who published the post in the first place.

Possible values: Friends, Only me, custom.

Default value: Friends.

Who sees tag suggestions when photos that look like you are uploaded?

When a friend publishes a photo that resembles the user, tagging suggestions can be shown to this friend to make the tagging process faster. This setting decides who can receive these suggestions.

Possible values: Friends, No one.

Default value: Friends.

Twitter

Photo tagging

Decides who on Twitter can tag the user in photos.

Possible values: Allow anyone, Only allow people I follow, Do not allow anyone.

Default setting: Allow anyone.

Protect my tweets

Makes the future tweets of the user protected, meaning that only a list of followers that the user has previously approved can see the published tweets.

Possible values: Enabled, Disabled.

Default value: Disabled.

Add a location to my tweets

Decides if the user wants to include their location when they publish a tweet.

Possible values: Enabled, Disabled.

Default value: Disabled.

Let others find me by my email address

Decides if other Twitter users can look the user up using their email address.

Possible values: Enabled, Disabled.

Default value: Enabled.

Let others find me by my phone number

Decides if other Twitter users can look the user up using their phone number.

Possible values: Enabled, Disabled.

Default value: Enabled.

Personalize ads

Decides if the user wants to see personalized ads on and off Twitter.

Possible values: Enabled, Disabled.

Default value: Enabled.

Personalize based on your apps

Decides if Twitter can see and store a list of the apps installed on the user's device and use this information to show more relevant content.

Possible values: Enabled, Disabled.

Default value: Disabled.

Personalize across all your devices

Decides whether the content should be personalized on all the used devices using the data linked to the account.

Possible values: Enabled, Disabled.

Default value: Enabled.

Personalize based on the places you've been

Decides if Twitter should use location information to show the user personalized content.

Possible values: Enabled, Disabled.

Default value: Enabled.

Track where you see Twitter content across the web

Decides if Twitter can track the websites the user visits that contain any Twitter element.

Possible values: Enabled, Disabled.

Default value: Disabled.

Share data through select partnerships

Decides if Twitter can share private data about the user (excluding name, email or phone number) with select partnerships.

Possible values: Enabled, Disabled.

Default value: Enabled.

Twitter for teams

Decides who can add the user to their team.

Possible values: Anyone, People I follow, Do not allow anyone.

Default value: Anyone.

Receive direct messages from anyone

Decides if people that the user doesn't follow can send them direct messages.

Possible values: Enabled, Disabled.

Default value: Disabled.

Send/receive read receipts

Decides whether other people in a conversation can see that the user has seen a message or not. Disabling receipts works both ways.

Possible values: Enabled, Disabled.

Default value: Enabled.

LinkedIn

Who can see your connections

Decides who on LinkedIn can see the user's list of connections.

Possible values: Only you, your connections.

Default value: Your connections.

Viewers of this profile also viewed

Decides whether this function should appear on the user's profile.

Possible values: Enabled, Disabled.

Default value: Enabled.

Sharing profile edits

Decides whether a user's network is notified when the user makes any changes to their profile.

Possible values: Enabled, Disabled.

Default value: Enabled.

Profile viewing options

When a user visits other people's profiles, they are notified of it. This setting decides how much information about the user they can view.

Possible values: Your name and headline, Private profile characteristics, Private mode.

Default value: Your name and headline.

Notifying connections when you're in the news

Decides if the connections of a user can be notified when the user is mentioned in an article or a blog post.

Possible values: Enabled, Disabled.

Default value: Enabled.

Who can see your last name

Decides whether the LinkedIn users that are not connected to the user can see their last name or just the initial.

Possible values: Show, Hide.

Default value: Show.

Who can follow you and see your public updates

Decides who can follow the user.

Possible values: Your connections, Everyone on LinkedIn.

Default value: Your connections.

Manage who can discover your profile from your email address

Decides who can find the user's profile by searching the email address in the search field.

Possible values: Everyone, 2-nd degree connections, Nobody.

Default value: Everyone.

Manage who can discover your profile from your phone number

Decides who can find the user's profile by searching the phone number in the search field.

Possible values: Everyone, 2-nd degree connections, Nobody.

Default value: Everyone.

Representing your organization

Decides if the user's picture and profile information can be shown on their employer's page.

Possible values: Enabled, Disabled.

Default value: Enabled.

Profile visibility off LinkedIn

Decides if the user's profile information can appear via partners and other services (for ex. Outlook).

Possible values: Enabled, Disabled.

Default value: Disabled.

Advertising preferences

Decides if LinkedIn should show the user interest based ads through their platform for third parties.

Possible values: Enabled, Disabled.

Default value: Disabled.

Google +

Who can send you notifications?

Decides whose actions should trigger a notification to the user.

Possible values: Anyone, Your circles, Extended circles, Only you.

Default value: Your circles.

Who can comment on your public posts?

Decides who on Google+ can comment on the user's public posts. People mentioned in posts could still be able to comment even if not part of this selection.

Anyone, Your circles, Extended circles, Only you.

Default value: Your circles.

Who can see your “+1 on posts” activity?

Decides who can see the posts the user has given +1 to.

Possible values: Anyone, Only you, Your circles, Custom.

Default value: Your circles.

Show geo location by default on newly shared Google+ albums

Decides if location information should be shared when the user publishes a new album.

Possible values: Enabled, Disabled.

Default value: Disabled.

Allow viewers to download my photos and videos shared on Google+

Decides if other users can download the photos and videos published by the user.

Possible values: Enabled, Disabled.

Default value: Enabled.

Don't feature my publicly shared Google+ photos as background images on Google products and services

Decides whether to prevent the user's public photos to be used as background for Google products and services.

Possible values: Enabled (don't use them), Disabled (use them).

Default value: Disabled (use them).

Help others discover my profile in search results

Decides if the user's profile can be found from search engines like Google.

Possible values: Enabled, disabled.

Default value: Enabled.

Show people who have added you to circles

Decides whether to show the people that have added the user to their circles on the profile.

Possible values: Enabled, Disabled.

Default value: Enabled.

Who can see the “People in your circles” section on your profile

Decides who can see the people that the user added to their circles.

Possible values: Only you, Public, your circles.

Default value: Public.

Pinterest

Search privacy – Hide your profile from search engines (ex: Google).

Decides whether to prevent the user's profile from being found by search engines.

Possible values: Enabled (hide from search engines), Disabled (visible from search engines).

Default value: Disabled.

Personalization - Use sites you visit to improve which recommendations and ads you see

Decides whether to use information about the websites the user has visited to personalize recommendations and ads.

Possible values: Enabled, Disabled.

Default value: Enabled.

Personalization - Use information from our partners to improve which recommendations and ads you see

Decides if the information that Pinterest receives from its partners can be used to improve ads and contents that are shown to the user.

Possible values: Enabled, Disabled.

Default value: Enabled.

B

Survey Questionnaire

Below are the questions asked in the survey questionnaire used for the exploratory study of chapter 4.

8/24/2017

Social Network Privacy Survey - Privacy settings on social networks

Privacy settings on social networks

Welcome to the survey on the privacy settings in common social network sites.

This survey is part of a master thesis I'm writing in Information management at the University of Fribourg.

All the data submitted is strictly anonymous

There are 57 questions in this survey

general questions

Gender *

Please choose **only one** of the following:

- Female
- Male

Age *

Choose one of the following answers

Please choose **only one** of the following:

- 1-18
- 19-30
- 31-50
- 51+

Occupation *

Choose one of the following answers

Please choose **only one** of the following:

- Student at University of Fribourg
- Other student
- Other

I have an account for the following social networks *

Check all that apply

Please choose **all** that apply:

- Facebook
- Twitter
- LinkedIn
- Google+
- Pinterest
- I don't have an account for any social network

Other:

[]How often do you use these social networks? *

Only answer this question if the following conditions are met:

Answer was 'Pinterest' or 'Google+' or 'LinkedIn' or 'Twitter' or 'Facebook' at question '4 [account]' (I have an account for the following social networks)

Please choose the appropriate response for each item:

	Hourly	Daily	Weekly	Monthly	Less often
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google+	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[]What do you use the social network(s) for mainly? *

Only answer this question if the following conditions are met:

((account_2.NAOK == "Y" or account_3.NAOK == "Y" or account_4.NAOK == "Y" or account_5.NAOK == "Y" or account_Fb.NAOK == "Y"))

	Stay in touch with friends	Stay up-to-date with news and current events	Fill up spare time	Share opinions	Share photos and videos	Other (please specify)
Facebook	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Twitter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LinkedIn	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Google +	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pinterest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Multiple answers possible

[]What do you use the social network(s) for mainly? (Specify) *

Only answer this question if the following conditions are met:

----- Scenario 1 -----

Answer was '1' at question '6 [use]' (What do you use the social network(s) for mainly?)

----- or Scenario 2 -----

Answer was '1' at question '6 [use]' (What do you use the social network(s) for mainly?)

----- or Scenario 3 -----

Answer was '1' at question '6 [use]' (What do you use the social network(s) for mainly?)

----- or Scenario 4 -----

Answer was '1' at question '6 [use]' (What do you use the social network(s) for mainly?)

----- or Scenario 5 -----

Answer was '1' at question '6 [use]' (What do you use the social network(s) for mainly?)

Facebook	<input type="text"/>
Twitter	<input type="text"/>
LinkedIn	<input type="text"/>
Google +	<input type="text"/>
Pinterest	<input type="text"/>

importance

[] I'm ok with giving personal information in exchange for a service *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
<input type="radio"/>				

[] It is important to know and be able to control who can see the information I share *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
<input type="radio"/>				

[]

I'm concerned that the information I submit could be used for "commercial purposes" *

Please choose the appropriate response for each item:

Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
<input type="radio"/>				

Commercial purposes includes mainly the fact of using the information to target ads or selling it to third parties to do the same

control

{} I know exactly who can see the information I share *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[]

I carefully choose the public for the information I share every time I publish something *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[]

The last time I reviewed my privacy settings was *

Please choose the appropriate response for each item:

	Last week	Last month	Last year	When I created the account	Never	Don't know
Facebook	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LinkedIn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Google +	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pinterest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

{} I've read the privacy policy of the following social networks *

Check all that apply

Please choose all that apply:

- Facebook
- Twitter
- LinkedIn
- Google +
- Pinterest
- None of them

Trust

[]

I trust the social network to choose the best default settings for the protection of my privacy *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[]

I am concerned that the information I publish on the social network could be misused *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

usability

[]

The privacy settings are easy to find *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

By privacy settings, we mean the "settings" page as well as the tools to control the audience for a post (if offered by the social network)

[]

I understand what every privacy setting does *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[]

I feel overwhelmed by the number of settings and I often think I forgot to set something important *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
LinkedIn	<input type="radio"/>				
Google +	<input type="radio"/>				
Pinterest	<input type="radio"/>				

[] To manage my privacy settings, I prefer to use

Please choose the appropriate response for each item:

	Website	Mobile website (smartphone / tablet)	Mobile App (smartphone / tablet)
Facebook	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LinkedIn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Google +	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pinterest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

defaults description

[]

Default privacy settings

In the next section, you will find a list of privacy settings present on the social networks you have an account for. Please select the settings that you think are applied by default when creating a new account.

default_fb**Facebook default privacy settings****[]Who can see your future posts?**

Choose one of the following answers

Please choose **only one** of the following:

- Public
- Friends
- Only me

[]Who can send you friend requests?

Choose one of the following answers

Please choose **only one** of the following:

- Everyone
- Friends of friends

[]Who can look you up using the email address you provided?

Choose one of the following answers

Please choose **only one** of the following:

- Everyone
- Friends of friends
- Friends

[]Who can look you up using the phone number you provided?

Choose one of the following answers

Please choose **only one** of the following:

- Everyone
- Friends of friends
- Friends

[]Do you want search engines outside of Facebook to link to your profile?

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

default_tw**Twitter default privacy settings****[]Photo tagging**

Choose one of the following answers

Please choose **only one** of the following:

- Allow anyone to tag me in photos
- Only allow people I follow to tag me in photos
- Do not allow anyone to tag me in photos

[]**Tweet privacy****Protect my tweets**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.

[]**Tweet location****Add a location to my Tweets**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet.

[]Discoverability

Please choose the appropriate response for each item:

	Yes	No
Let others find me by my email address	<input type="radio"/>	<input type="radio"/>
Let others find me by my phone number	<input type="radio"/>	<input type="radio"/>

[]Personalization

Choose one of the following answers

Please choose **only one** of the following:

- Track
- Do Not Track

While you have Do Not Track turned on, your visits to sites that feature Twitter are not available to personalize your experience.

[]

Promoted content

Tailor ads based on information shared by ad partners

Choose one of the following answers

Please choose **only one** of the following:

- Track
- Do not track

This lets Twitter display ads about things you've already shown interest in.

[]

Twitter for teams

Choose one of the following answers

Please choose **only one** of the following:

- Allow anyone to add me to their team
- Only allow people I follow to add me to their team
- Do not allow anyone to add me to their team

[]Direct messages

Please choose the appropriate response for each item:

	Yes	No
Receive direct messages from anyone	<input type="radio"/>	<input type="radio"/>
Send/receive read receipts	<input type="radio"/>	<input type="radio"/>

default_lk**LinkedIn default privacy settings**

[]

Who can see your connections**Choose who can see your list of connections**

Choose one of the following answers

Please choose **only one** of the following:

- Only you
- Your connections

[]

How you rank**Choose whether or not to be included in this feature**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

How You Rank shows how you compare to your connections and colleagues in terms of profile views. If you turn this feature off, others won't see you or your standings in their How You Rank page. You also won't see your own rank or get tips on improving your visibility.

[]

Viewers of this profile also viewed**Choose whether or not this feature appears when people view your profile**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Should we display "Viewers of this profile also viewed" box on your Profile page?

[]

Sharing profile edits**Choose whether your network is notified about profile changes**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Should we let people know when you change your profile, make recommendations, or follow companies?

[]

Profile viewing options**Choose whether you're visible or viewing in private mode**

Choose one of the following answers

Please choose **only one** of the following:

- Your name and headline
- Private profile characteristics
- Private mode

[]

Notifying connections when you're in the news**Choose whether we notify people in your network that you've been mentioned in an article or blog post**

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

[]

Followers**Choose who can follow you and see your public updates**

Choose one of the following answers

Please choose **only one** of the following:

- Everyone on LinkedIn
- Your connections

Choosing "Everyone" lets people outside your network follow your public updates.

[]

Suggesting you as connection based on your email address**Choose who can see you as a suggested connection if they have your email address**

Choose one of the following answers

Please choose **only one** of the following:

- Everyone on LinkedIn
- 2nd-degree connections
- Nobody

People can upload their contacts to LinkedIn to discover potential connections. If someone has your email address in their contacts, we may suggest they invite you to connect – it's your choice whether or not to accept.

[]

Suggesting you as a connection based on your phone number**Choose who can see you as suggested connection if they have your phone number**

Choose one of the following answers

Please choose **only one** of the following:

- Everyone on LinkedIn
- 2nd-degree connections
- Nobody

[]

Representing your organization

Choose if we can show your profile information on your employers's pages

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Hide my picture and profile information from showing up in this section of a job detail page?

[]

Sharing data with third parties

Choose if we can share your basic profile data with third parties

Please choose the appropriate response for each item:

	Yes	No
Should we share your basic profile and contact information with third party applications?	<input type="radio"/>	<input type="radio"/>
Should we allow your contact information to be shared with trusted third party platforms?	<input type="radio"/>	<input type="radio"/>

[]

Advertising preferences

Choose whether LinkedIn can use cookies to personalize ads

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

default_g+**Google+ default privacy settings****[]General**

Please choose the appropriate response for each item:

	Anyone	Your circles	Extended circles	Only you
Who can send you notifications?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Who can comment on your public posts?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[]Who can see your "+1's on posts" activity?

Choose one of the following answers

Please choose **only one** of the following:

- Anyone
- Only you

[]Photos and Videos shared on Google+

Please choose the appropriate response for each item:

	Yes	No
Show geo location by default on newly shared Google+ albums	<input type="radio"/>	<input type="radio"/>
Allow viewers to download my photos and videos shared on Google+	<input type="radio"/>	<input type="radio"/>
Don't feature my publicly-shared Google+ photos as background images on google products and services	<input type="radio"/>	<input type="radio"/>

[]Profile

Please choose the appropriate response for each item:

	Yes	No
Show how many times your profile and content have been viewed	<input type="radio"/>	<input type="radio"/>
Show your Google+ Communities posts on your profile	<input type="radio"/>	<input type="radio"/>
Help others discover my profile in search results	<input type="radio"/>	<input type="radio"/>
Show people who have added you to circles	<input type="radio"/>	<input type="radio"/>

[]Show these profile tabs to visitors (they're always visible to you)

Check all that apply

Please choose **all** that apply:

- Photos
- Youtube/videos
- +1
- Reviews

[]Who can see the "people in your circles" section on your profile

Choose one of the following answers

Please choose **only one** of the following:

- Only you
- Public
- Your circles

default_pin**Pinterest default privacy settings**

[] Hide your profile from search engines (ex:Google).

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

[] Use sites you visit to improve which recommendations and ads you see

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

[] Use information from our partners to improve which recommendations and ads you see.

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

no sns

]*In the previous question you said that you don't have an account for any of the listed social networks. Why?*

Only answer this question if the following conditions are met:

Answer was 'I don't have an account for any social network' at question '4 [account]' (I have an account for the following social networks)

Choose one of the following answers

Please choose **only one** of the following:

- I'm not interested in social network sites
- I don't understand how to use them
- I don't want to share my personal information on the internet
- No answer

end

[]

You reached the end of the questionnaire. Please click on the "submit" button below to send it or click on "previous" to go back and modify your answers.

C

Survey results

Below are is the SPSS output of the analyses performed on the results of the survey performed for the exploratory study in chapter 4.

Starting language

		Frequency	Percent	Valid Percent	Cumulative
					Percent
Valid	de	3	3.4	3.4	3.4
	en	54	62.1	62.1	65.5
	fr	10	11.5	11.5	77.0
	it	20	23.0	23.0	100.0
	Total	87	100.0	100.0	

Gender

		Frequency	Percent	Valid Percent	Cumulative
					Percent
Valid	Female	53	60.9	60.9	60.9
	Male	34	39.1	39.1	100.0
	Total	87	100.0	100.0	

Age

				Cumulative Percent
	Frequency	Percent	Valid Percent	
Valid	1-18	1	1.1	1.1
	19-30	73	83.9	83.9
	31-50	11	12.6	97.7
	51+	2	2.3	100.0
	Total	87	100.0	100.0

Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Student at University of Fribourg	42	48.3	67.7	67.7
	Other student	20	23.0	32.3	100.0
	Total	62	71.3	100.0	
Missing	System	25	28.7		
	Total	87	100.0		

[Other] Occupation

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	65	74.7	74.7	74.7
	CEO	1	1.1	1.1
	Ceo, sensory scientist lab manager	1	1.1	1.1
	Dipendente	1	1.1	1.1
	Dipendente statale	1	1.1	1.1
	Docente scuola speciale	1	1.1	1.1
	Employee	1	1.1	1.1
	Étudiant à HES-SO, Fribourg	1	1.1	1.1
	Étudiante en emploi	1	1.1	1.1
	Impiegata	1	1.1	1.1

impiegato	1	1.1	1.1	86.2
JMCS	1	1.1	1.1	87.4
Lavoratore	1	1.1	1.1	88.5
Office employee	1	1.1	1.1	89.7
Operaio	2	2.3	2.3	92.0
Paralegal	1	1.1	1.1	93.1
PhD	1	1.1	1.1	94.3
Post-doc	1	1.1	1.1	95.4
Postdoc	1	1.1	1.1	96.6
Professor	1	1.1	1.1	97.7
researcher	1	1.1	1.1	98.9
Stagiaire	1	1.1	1.1	100.0
Total	87	100.0	100.0	

I have an account for the following social networks

Facebook	83
Twitter	27
LinkedIn	31
Google +	30
Pinterest	25
Other (please specify)	59
Deviantart and tumblr	1
Instagram	14
Instagram , Snapchat	1
Instagram et snapchat	1
Instagram, Snapchat	1
Instagram,Shutterstock,	1
Instagram; Snapchat	1
Reddit	1
snap chat	1
Snapchat	3
tumblr	1
Tumblr	1
Tumblr, Instagram	1

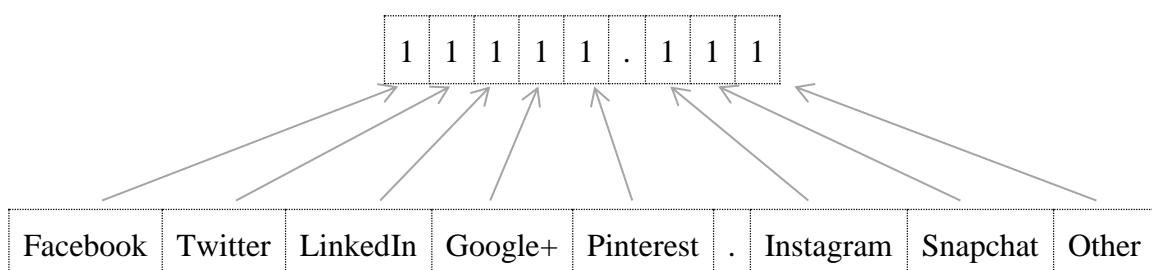
I don't have an account for any social network	2
---------------------------------------------------	---

Number of accounts per person

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	21	24.1	24.7	24.7
	2.00	32	36.8	37.6	62.4
	3.00	20	23.0	23.5	85.9
	4.00	9	10.3	10.6	96.5
	5.00	3	3.4	3.5	100.0
	Total	85	97.7	100.0	
Missing	System	2	2.3		
Total		87	100.0		

Social Network account combinations:

The following numbers are composed by a series of binary variables where 1 means that the user has an account for the specific social network and 0 that they don't. The number is made as follows:



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	100.000	1	1.1	1.2	1.2
	1100.000	1	1.1	1.2	2.4
	10000.000	18	20.7	21.2	23.5

10000.010	1	1.1	1.2	24.7
10000.101	1	1.1	1.2	25.9
10001.000	6	6.9	7.1	32.9
10001.010	1	1.1	1.2	34.1
10001.100	1	1.1	1.2	35.3
10001.110	1	1.1	1.2	36.5
10010.000	6	6.9	7.1	43.5
10010.010	1	1.1	1.2	44.7
10010.100	1	1.1	1.2	45.9
10011.100	2	2.3	2.4	48.2
10100.000	5	5.7	5.9	54.1
10100.010	1	1.1	1.2	55.3
10100.100	3	3.4	3.5	58.8
10100.110	1	1.1	1.2	60.0
10101.000	3	3.4	3.5	63.5
10101.100	1	1.1	1.2	64.7
10101.101	1	1.1	1.2	65.9
10110.000	1	1.1	1.2	67.1
10110.100	1	1.1	1.2	68.2
10111.000	1	1.1	1.2	69.4
11000.000	3	3.4	3.5	72.9
11000.100	1	1.1	1.2	74.1
11001.000	3	3.4	3.5	77.6
11001.001	1	1.1	1.2	78.8
11010.000	2	2.3	2.4	81.2
11010.001	2	2.3	2.4	83.5
11010.100	1	1.1	1.2	84.7
11010.110	1	1.1	1.2	85.9
11011.100	1	1.1	1.2	87.1
11100.000	1	1.1	1.2	88.2
11110.000	5	5.7	5.9	94.1
11110.100	1	1.1	1.2	95.3
11110.110	1	1.1	1.2	96.5
11111.000	1	1.1	1.2	97.6
11111.001	1	1.1	1.2	98.8
11111.100	1	1.1	1.2	100.0

Total	85	97.7	100.0	
Missing System	2	2.3		
Total	87	100.0		

How often do you use these social networks?

	Hourly	Daily	Weekly	Monthly	Less often
Facebook	26.5%	67.5%	3.6%	0.0%	2.4%
Twitter	3.7%	22.2%	22.2%	18.5%	33.3%
LinkedIn	0.0%	16.1%	45.2%	25.8%	12.9%
Google+	0.0%	6.7%	10.0%	13.3%	70.0%
Pinterest	0.0%	12.0%	28.0%	20.0%	40.0%

What do you use the social networks for?

	Stay up-to-date with news and current events				Fill up spare time				Share opinions				Share photos and videos				Other	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Facebook	60	72.3%	54	65.1%	51	61.4%	11	13.3%	25	30.1%	3	3.6%						
Twitter	3	11.1%	18	66.7%	6	22.2%	7	25.9%	0	0.0%	5	18.5%						
LinkedIn	6	19.4%	11	35.5%	2	6.5%	1	3.2%	0	0.0%	18	58.1%						
Google+	3	10.0%	4	13.3%	6	20.0%	1	3.3%	1	3.3%	15	50.0%						
Pinterest	0	0.0%	4	16.0%	6	24.0%	0	0.0%	6	24.0%	12	48.0%						

What do you use the social networks for? (other -> specify)

Facebook	Me renseigner sur les autres, comprendre leur vision personnelle et les perceptions globales sur le contexte politique et social. Parfois pour les flirts. Pour gérer mes événements
	Not used.
	Follow funny pages and see what other people do
Twitter	Bookmark relevant things by listing them
	get status information of content creators
	Traffic information
	Never use it
	Participer à des concours
LinkedIn	As a kind of public personal page to share my work information
	Look for job offers
	Create job network
	Développer le réseau, être visible
	élargir mon réseau professionnel
	Extension des réseaux professionnels
	Find a job
	follow career development of former colleagues/students
	Job search
	Job
	Networking (Different from staying in touch with friends)
	Nothing at the moment
	Job opportunities
	Professional networking
	Professionnel
Google+	When I was unemployed, searching a job
	Easy signup
	I don't use it very much. I have it just because I have a gmail account :)

	I just have it..
	I never use it
	Je n'y vais jamais
	Works in google maps
	Mails
	mainly for google drive
	No use
	Never use it
	Almost never use it
	Not used.
	Nothing
	Nothing, I have it only because I use gmail
	Nothing, it just exists because I have a Google account
Pinterest	Check recipes
	Get inspiration
	I created an account once to pin links interested to a certain research topic. Then quickly quit using it.
	Job
	M'inspirer pour des coiffures, décos, recettes, etc.
	Find new ideas
	Find ideas
	Search of school material, activity ideas, ...
	To get some inspirations
	Trouver des idées de bricolage
	Find ideas and inspirations
	Work ideas

3 questions

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
I'm ok with giving personal information in exchange for a service	21.2%	40.0%	14.1%	22.4%	2.4%	100.0%
It is important to know and be able to control who can see the information I share	0.0%	4.7%	0.0%	30.6%	64.7%	100.0%
I'm concerned that the information I submit could be used for "commercial purposes"	7.1%	12.9%	11.8%	42.4%	25.9%	100.0%

I know exactly who can see the information I share

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	8.4%	19.3%	8.4%	50.6%	13.3%	100.0%
Twitter	7.4%	22.2%	25.9%	22.2%	22.2%	100.0%
LinkedIn	9.7%	22.6%	41.9%	16.1%	9.7%	100.0%
Google+	6.7%	23.3%	43.3%	13.3%	13.3%	100.0%
Pinterest	4.0%	20.0%	40.0%	32.0%	4.0%	100.0%

I carefully choose the public for the information I share every time I publish something

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	3.6%	15.7%	3.6%	38.6%	38.6%	100.0%
Twitter	3.7%	18.5%	18.5%	44.4%	14.8%	100.0%
LinkedIn	3.2%	19.4%	25.8%	29.0%	22.6%	100.0%
Google+	10.0%	3.3%	46.7%	20.0%	20.0%	100.0%
Pinterest	4.0%	20.0%	48.0%	20.0%	8.0%	100.0%

The last time I reviewed my privacy settings was

	Last week	Last month	Last year	When I created the account	Never	Don't know	Total
Facebook	15.7%	49.4%	20.5%	10.8%	0.0%	3.6%	100.0%
Twitter	3.7%	18.5%	22.2%	25.9%	25.9%	3.7%	100.0%
LinkedIn	6.5%	19.4%	16.1%	45.2%	6.5%	6.5%	100.0%
Google+	6.7%	10.0%	6.7%	40.0%	20.0%	16.7%	100.0%
Pinterest	4.0%	4.0%	8.0%	32.0%	44.0%	8.0%	100.0%

I've read the privacy policy of the following social networks

	Last week	Last month
Facebook	31	36.47%
Twitter	3	3.53%
LinkedIn	5	5.88%
Google+	3	3.53%
Pinterest	1	1.18%
None of them	53	62.35%

I trust the social network to choose the best default settings for the protection of my privacy

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	34.9%	38.6%	13.3%	12.0%	1.2%	100.0%
Twitter	14.8%	37.0%	18.5%	25.9%	3.7%	100.0%
LinkedIn	9.7%	22.6%	22.6%	41.9%	3.2%	100.0%
Google+	16.7%	36.7%	33.3%	10.0%	3.3%	100.0%
Pinterest	16.0%	24.0%	48.0%	8.0%	4.0%	100.0%

I am concerned that the information I publish on the social network could be misused

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	1.2%	8.4%	20.5%	48.2%	21.7%	100.0%
Twitter	11.1%	14.8%	25.9%	40.7%	7.4%	100.0%
LinkedIn	3.2%	22.6%	22.6%	38.7%	12.9%	100.0%
Google+	6.7%	3.3%	36.7%	36.7%	16.7%	100.0%
Pinterest	4.0%	16.0%	52.0%	24.0%	4.0%	100.0%

The privacy settings are easy to find

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	1.2%	16.9%	7.2%	66.3%	8.4%	100.0%
Twitter	0.0%	14.8%	48.1%	29.6%	7.4%	100.0%
LinkedIn	0.0%	12.9%	38.7%	38.7%	9.7%	100.0%
Google+	3.3%	10.0%	53.3%	33.3%	0.0%	100.0%
Pinterest	0.0%	16.0%	68.0%	12.0%	4.0%	100.0%

I understand what every privacy setting does

	Strongly disagree	Disagree	Don't know	Agree	Strongly Agree	Total
Facebook	8.4%	24.1%	21.7%	38.6%	7.2%	100.0%
Twitter	0.0%	14.8%	48.1%	37.0%	0.0%	100.0%
LinkedIn	3.2%	12.9%	41.9%	35.5%	6.5%	100.0%
Google+	0.0%	13.3%	56.7%	20.0%	10.0%	100.0%
Pinterest	8.0%	8.0%	64.0%	20.0%	0.0%	100.0%

I feel overwhelmed by the number of settings and I often think I forgot to set something important

Facebook	10.8%	27.7%	14.5%	41.0%	6.0%	100.0%
Twitter	11.1%	22.2%	55.6%	11.1%	0.0%	100.0%
LinkedIn	12.9%	32.3%	32.3%	22.6%	0.0%	100.0%
Google+	10.0%	16.7%	66.7%	3.3%	3.3%	100.0%
Pinterest	8.0%	4.0%	68.0%	16.0%	4.0%	100.0%

To manage my privacy settings, I prefer to use

	Website	Mobile website (smartphone / tablet)	Mobile App (smartphone / tablet)	Total
Facebook	81.9%	0.0%	18.1%	100.0%
Twitter	66.7%	3.7%	29.6%	100.0%
LinkedIn	87.1%	0.0%	12.9%	100.0%
Google+	83.3%	3.3%	13.3%	100.0%
Pinterest	68.0%	0.0%	32.0%	100.0%

Default privacy settings

Here are the results of the Default settings section of the questionnaire. In the following tables are indicated the right answers on the first column, the part of wrong answers that led to oversharing on the second and the part that led to undersharing in the third column.

Facebook

	Right answers	Oversharing	Undersharing
Mean	0.479518	0.76506	0.189759
Standard Error	0.023489	0.036703	0.033359
Median	0.4	1	0
Mode	0.4	1	0
Standard Deviation	0.213997	0.334385	0.303913
Sample Variance	0.045795	0.111813	0.092363
Kurtosis	-0.32693	0.680381	1.767014
Skewness	0.548883	-1.35186	1.628329
Range	0.8	1	1
Minimum	0.2	0	0
Maximum	1	1	1
Sum	39.8	63.5	15.75
Count	83	83	83

Twitter

	Right answers	Oversharing	Undersharing
Mean	0.496296	0.564727	0.435273
Standard Error	0.021669	0.063024	0.063024
Median	0.5	0.666667	0.333333
Mode	0.5	0	1
Standard Deviation	0.112597	0.327482	0.327482
Sample Variance	0.012678	0.107244	0.107244
Kurtosis	0.794507	-0.83879	-0.83879
Skewness	-0.44626	-0.47661	0.476609
Range	0.5	1	1
Minimum	0.2	0	0
Maximum	0.7	1	1

Sum	13.4	15.24762	11.75238
Count	27	27	27

LinkedIn

	Right answers	Oversharing	Undersharing
Mean	0.489744	0.857685	0.142315
Standard Error	0.03566	0.045756	0.045756
Median	0.461538	1	0
Mode	0.307692	1	0
Standard Deviation	0.195317	0.250618	0.250618
Sample Variance	0.038149	0.06281	0.06281
Kurtosis	-0.80216	3.464034	3.464034
Skewness	0.153149	-1.8993	1.899303
Range	0.769231	1	1
Minimum	0.076923	0	0
Maximum	0.846154	1	1
Sum	14.69231	25.73056	4.269444
Count	30	30	30

Google+

	Right answers	Oversharing	Undersharing
Mean	0.442857	0.671216	0.26618
Standard Error	0.026442	0.058573	0.057249
Median	0.4	0.714286	0.242857
Mode	0.3	1	0
Standard Deviation	0.139917	0.309937	0.268521
Sample Variance	0.019577	0.096061	0.072104
Kurtosis	-1.03704	-0.32701	1.275084
Skewness	0.288856	-0.74769	1.114916
Range	0.5	1	1
Minimum	0.2	0	0
Maximum	0.7	1	1
Sum	12.4	18.79405	5.855952
Count	28	28	22

Pinterest

	Right answers	Oversharing	Undersharing
Mean	0.578947	0.526316	0
Standard Error	0.101458	0.117688	0
Median	0.666667	1	0
Mode	1	1	0
Standard Deviation	0.442246	0.512989	0
Sample Variance	0.195582	0.263158	0
Kurtosis	-1.83016	-2.23529	#DIV/0!
Skewness	-0.2563	-0.11467	#DIV/0!
Range	1	1	0
Minimum	0	0	0
Maximum	1	1	0
Sum	11	10	0
Count	19	19	25

D

Prototype test wizard screens

Below are the screenshots of the different screens of the wizard used to guide the users through the usability test of the three interfaces for the Privacy Dashboard.

The screenshot shows a prototype test wizard interface for a 'Social Network Privacy Dashboard'. At the top, there is a horizontal navigation bar with eleven icons: play, speech bubble, download, info, laptop, speech bubble, laptop, speech bubble, laptop, speech bubble, and a checkmark. Below this is a title bar with the text 'Social Network Privacy Dashboard Prototype test'. The main content area is divided into three columns:

- What is this?**

For my master thesis, I have developed a prototype for a tool called Privacy Dashboard. Its goal is to give people a quick way to check the state of their privacy on different social networks. What I need to do now, is to test this prototype and gather information about its usability and usefulness from actual potential users.
- How does it work?**

During this test, after the preparation phase, you will have to use the tool to accomplish a given list of tasks and answer some questions regarding the experience. The test includes 3 different interfaces for you to test. To be able to analyse the results afterwards, I will record what you do on the screen and (if you give me permission in the next steps) audio from your microphone and video from your webcam.
- Privacy policy**
 - No access to any of your social network accounts is required or asked.
 - All the information gathered during this test will only be used for the purpose of evaluating the prototype.
 - Audio and webcam recordings (if you choose to provide them) will not be shared with anyone and will be deleted after the finish of my master thesis.

A red button at the bottom center of the content area says 'Let's start!'



First some info about you

Don't forget to click "Submit" before going to the next page

How old are you?*

Gender *

Male Female

Privacy importance * ⓘ

How concerned do you consider yourself about
your privacy on social networks, on a scale from



Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



In my opinion, a social network's privacy policy defines: *

- What information the other social network users can see about me
- What information the social network can collect about me and what they do with it
- I don't know

How often do you use/visit the following social networks?*

	Hourly	Daily	Weekly	Monthly	Less often	I don't have an account
Facebook	<input type="radio"/>					
Twitter	<input type="radio"/>					
LinkedIn	<input type="radio"/>					
Google+	<input type="radio"/>					
Pinterest	<input type="radio"/>					

Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



How often do you POST something on the following social networks? *

	Hourly	Daily	Weekly	Monthly	Less often	I don't have an account
Facebook	<input type="radio"/>					
Twitter	<input type="radio"/>					
LinkedIn	<input type="radio"/>					
Google+	<input type="radio"/>					
Pinterest	<input type="radio"/>					

When was the last time you checked your privacy settings? *

	Last week	Last month	Last year	When creating the account	Never
Facebook	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
... ..	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

[next](#)



When was the last time you checked your privacy settings? *

	Last week	Last month	Last year	When creating the account	Never
Facebook	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LinkedIn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Google+	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pinterest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Powered by formsite

[SUBMIT](#)

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

[next](#)



Let's prepare!

1.

To be able to observe and record what you do, I need you to launch a little program called Teamviewer QS. Please download it from the link below and run it. Once started, you will see your personal ID and Password, like in the picture here. Please fill them in here and click submit, so that I can connect with your computer and we can start.

For Windows:

Download

For Mac:

Download

For Ubuntu/Debian:

Download (requires full installation)

2.



3.

Please select what I can record: *

Your ID *

Your Pass *

SUBMIT

Powered by Cognito Forms.
LOAD.COM

Don't forget to click "**SUBMIT**" before going to the next page

[Previous](#)

[next](#)



Scenario

Your name is Jack and you have accounts for multiple social networks. You had a discussion about the privacy on social networks with a friend and you decided to inform yourself and check your profiles. To do that, you are going to use a tool he told you about called Privacy Dashboard

What do you have to do?

Watch this short tutorial: [Video tutorial](#)

- If the microphone is active, please try to say out loud what you are doing, it is very helpful for the analysis afterwards.
- When answering the post-test questions, please be honest. There are no right or wrong answers. I don't look while you fill in the questionnaires.
- Feel free to write the answers in Italian, French or German if you prefer.

[Previous](#) [next](#)

Note: the video tutorial can be found on YouTube at the following address: https://youtu.be/pJhzp_yoYWg



1.

Click this button to open the Privacy Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

2.

Find out if your Pinterest profile can be found from search engines

Compare the settings responsible for personalising the ads you see on LinkedIn and Twitter to see if you set the same value for both.

Check what could happen if you set "who can see your future posts" to **Public** on Facebook

Is there a public post that your boss shouldn't see on your Facebook profile?

What data does Google + collect about you?

[Previous](#)

[next](#)



Click this button to open the Privacy Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

Find out if your Pinterest profile can be found from search engines

Compare the settings responsible for personalising the ads you see on LinkedIn and Twitter to see if you set the same value for both.

Check what could happen if you set "who can see your future posts" to **Public** on Facebook

Is there a public post that your boss shouldn't see on your Facebook profile?

What data does Google + collect about you?

Check if all your privacy settings on Pinterest correspond to the recommended value

Click on "Finish test" on the left (on the Privacy Dashboard)

[Previous](#)

[next](#)



About this interface

Don't forget to click "Submit" before going to the next page

Please answer the questions below about the interface you just tested *

	Very Difficult	Difficult	Average	Easy	Very Easy
How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				

Did you like / dislike something in particular?

Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



	Very Difficult	Difficult	Average	Easy	Very Easy
How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				

Did you like / dislike something in particular?

Powered by 

SUBMIT

Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



1.

Click this button to open the Privacy Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

2.

Find out if your LinkedIn connections can be notified when you are on the news

Find out if Twitter can collect information about you even when you are not on their website

Check if there is a public picture on Facebook that you wouldn't want to be public

Check what "Help others discover my profile in search results" on Google+ does

Find out the default value for "Personalize ads" on Twitter

Check who can see your friend/connections list on Facebook and LinkedIn to see if you set an equivalent value for both settings

[Previous](#)

[next](#)



Click this button to open the Privacy Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

Find out if your LinkedIn connections can be notified when you are on the news

Find out if Twitter can collect information about you even when you are not on their website

Check if there is a public picture on Facebook that you wouldn't want to be public

Check what "Help others discover my profile in search results" on Google+ does

Find out the default value for "Personalize ads" on Twitter

Check who can see your friend/connections list on Facebook and LinkedIn to see if you set an equivalent value for both settings

Click on "Finish test" on the left (on the Privacy Dashboard)

[Previous](#)

[next](#)



About this interface

Don't forget to click "Submit" before going to the next page

Please answer the questions below about the interface you just tested *

Very Difficult Difficult Average Easy Very Easy

How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
---------------------------------------------------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				
--------------------------------------------------------------------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Did you like / dislike something in particular?

Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



Very Difficult Difficult Average Easy Very Easy

How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
---------------------------------------------------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				
--------------------------------------------------------------------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Did you like / dislike something in particular?

Powered by

SUBMIT

Don't forget to click "**SUBMIT**" at the end of the questionnaire **before** going to the next page

[Previous](#)

[next](#)



1.

Click this button to open the Privacy Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

2.

Find out who can tag you in photos on Twitter

Find out what "Don't feature my publicly shared Google+ photos as background images on Google products and services" does on Google+

Check what could happen if people can look you up using your phone number on Facebook

Check if the information that Facebook collects about you can be shared with companies outside of the Facebook group

Compare the settings responsible for being found by search engines on Google+ and Pinterest

[Previous](#)

[next](#)



Dashboard and try to accomplish the listed tasks, one by one

[Open Privacy Dashboard ↗](#)

Find out what "Don't feature my publicly shared Google+ photos as background images on Google products and services" does on Google+

Check what could happen if people can look you up using your phone number on Facebook

Check if the information that Facebook collects about you can be shared with companies outside of the Facebook group

Compare the settings responsible for being found by search engines on Google+ and Pinterest to see if you set the same value for both.

Check how private / public your profile is on Google +

Click on "Finish test" on the left (on the Privacy Dashboard)

[Previous](#)

[next](#)



About this interface

Don't forget to click on "Submit" before going to the next page

Please answer the questions below about the interface you just tested *

	Very Difficult	Difficult	Average	Easy	Very Easy
How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				

Did you like / dislike something in particular?

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

[next](#)



	Very Difficult	Difficult	Average	Easy	Very Easy
How easy was it to accomplish the tasks using this interface?	<input type="radio"/>				
How easy was it to see the differences / similarities between social networks?	<input type="radio"/>				

Did you like / dislike something in particular?

Powered by 

SUBMIT

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

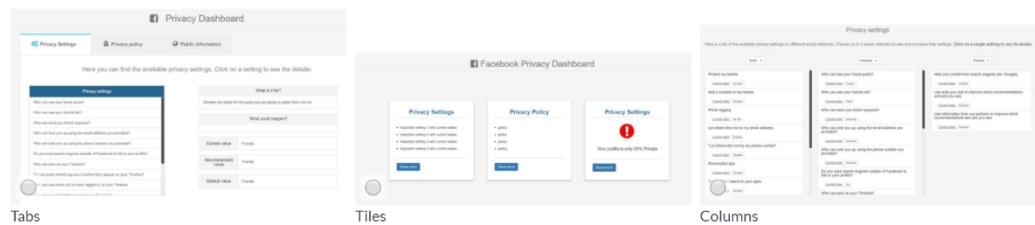
[next](#)



About the Privacy Dashboard in general

Don't forget to click "Submit" before going to the next page

Which interface did you like the most? *



Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

[next](#)



Did you like or dislike a part of the prototype in particular? ⓘ

Please rate the following statements *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The tool provides useful information about privacy on social networks	<input type="radio"/>				
The privacy assessment (see picture) of the profile was useful	<input type="radio"/>				
The tool made me think more about privacy on social networks	<input type="radio"/>				



Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page

[Previous](#)

[next](#)



Please rate the following statements *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The tool provides useful information about privacy on social networks	<input type="radio"/>				
The privacy assessment (see picture) of the profile was useful	<input type="radio"/>				
The tool made me think more about privacy on social networks	<input type="radio"/>				
I learned something I didn't know before using this tool	<input type="radio"/>				
If it was available, I would use it	<input type="radio"/>				



Do you have any other comments about the prototype you just tested?

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page [Previous](#) [next](#)



networks

I learned something I didn't know before using this tool	<input type="radio"/>				
If it was available, I would use it	<input type="radio"/>				



Do you have any other comments about the prototype you just tested?

Powered by formsite

SUBMIT

Don't forget to click "SUBMIT" at the end of the questionnaire before going to the next page [Previous](#) [next](#)



And we're finished!

Thank you very much for your participation, your help is really appreciated

If you have anything else you want to add about the prototype or the testing experience in general, feel free to use this box.

[Report abuse](#)

Powered by formsite

SUBMIT

E

Test tasks

Below is a list of the tasks that the participants had to accomplish for each interface, with a short description of the actions that they should have accomplished. Every set is composed by three tasks concerning the list of privacy settings, one about the privacy policy, one about the public information and one about the comparison between social networks.

Interface 1 – Tabs

- Find out if your Pinterest profile can be found from search engines.
The user should select Pinterest on the left and look for “Hide your profile from search engines (ex. Google) on the privacy settings list to check the current value.
- Compare the settings responsible for personalizing the ads you see on LinkedIn and Twitter to see if you set the same value for both.
The user should select LinkedIn on the left and look for “Advertising preferences” on the list of privacy setting to check the current value. They should than select Twitter and look for “Personalize ads” to see if the current value is equivalent to the one set on LinkedIn.
- Check what could happen if you set “who can see your future posts” to Public on Facebook.
The user should select Facebook on the left and then look for “who can see your future posts” on the list of privacy settings to read what is written under the “What could happen” section.
- Is there a public post that your boss shouldn’t see on your Facebook profile?
The user should click on the “Public information” tab of the Facebook section and look under “Public posts” to see if there is a post that their boss shouldn’t see.
- What data does Google+ collect about you?
The user should select Google+ on the left and go to the “Privacy Policy” section, to see what information the social network can collect about them, under “What info do they collect?”.
- Check if all your privacy settings on Pinterest correspond to the recommended value.
The user should select Pinterest on the left and check, one by one, the three privacy settings on the Pinterest list to see if the field “current value” corresponds to “recommended value”.

- Click on “Finish test” on the left (on the Privacy Dashboard).

The user should click on “Finish Test” on the left to close the tab and go back to the wizard. This step is not evaluated since it is not really part of the application.

Interface 2 -Tiles

- Find out if your LinkedIn connections can be notified when you are on the news.
The user should select LinkedIn on the left, click on “show more” on the Privacy settings tile and look for “Notifying connections when you’re in the news” in the list of settings to check the current value.
- Find out if Twitter can collect information about you even when you are not on their website.
The user should select Twitter on the left and click on “show more” on the Privacy Policy tile, to check under “what info do they collect” and find “interaction with external services”.
- Check if there is a public picture on Facebook that you wouldn’t want to be public.
The user should select Facebook on the left, click on “show more” on the Public Information tile and look at the pictures shown to see if there is anything that shouldn’t be public.
- Check what “Help others discover my profile in search results” on Google+ does.
The user should select Google+ on the left and click on “show more” on the Privacy settings tile to see the list of privacy settings. They should then look for “Help others discover my profile in search results” and see what is written in the “what is it for” section.
- Find out the default value for “Personalize ads” on Twitter.
The user should select Twitter on the left, click on “show more” and look for the “Personalize ads” setting in the list to check the current value.
- Check who can see your friend/connections list on Facebook and LinkedIn to see if you set an equivalent value for both settings.
The user should select Facebook on the left, click on “show more” in the privacy settings tile and look for the current value of “Who can see your friend list”. They should then select LinkedIn on the left and either see the current value of “Who can see your connections” on the preview or click on “Show more” and look for in the complete list of privacy settings.
- Click on “Finish test” on the left (on the Privacy Dashboard).
The user should click on “Finish Test” on the left to close the tab and go back to the wizard. This step is not evaluated since it is not really part of the application.

Interface 3 – Columns

- Find out who can tag you in photos on Twitter.

The user should select Twitter using one of the three dropdown menus and then look for the “Photo tagging” setting to see the current state.

- Find out what “Don’t feature my publicly shared Google+ photos as background images on Google products and services” does on Google+.

The user should select Google+ using one of the three dropdown menus and then look for the “Don’t feature my publicly shared Google+ photos as background images on Google products and services” setting on the list. By clicking on the setting the user can see the details, including the purpose of the privacy setting.

- Check what could happen if people can look you up using your phone number on Facebook.

The user should select Facebook using one of the three dropdown menus and then look for the “Who can look you up using the phone number you provided” setting on the list. By clicking on the setting the user can see the details, including an example of what could happen if it was set to public.

- Check if the information that Facebook collects about you can be shared with companies outside of the Facebook group.

The user should select “privacy policy” on the left and then use one of the three dropdown menus to select Facebook. Under “Who can they share it with” they will see that their information can be shared for example with vendors or service providers.

- Compare the settings responsible for being found by search engines on Google+ and Pinterest to see if you set the same value for both.

The user should select “privacy settings” on the left and then use one of the three dropdowns to select Google+ and another to select Pinterest. They should then find “Help others discover my profile in search results” for Google+ and “Hide your profile from search engines (ex: Google)” for Pinterest, to be able to compare the two current values.

- Check how private/ public your profile is on Google +.

The user should select “Public information” on the left and then use one of the three dropdown menus to select “Google+” and see that the profile is 70% private.

- Click on “Finish test” on the left (on the Privacy Dashboard).

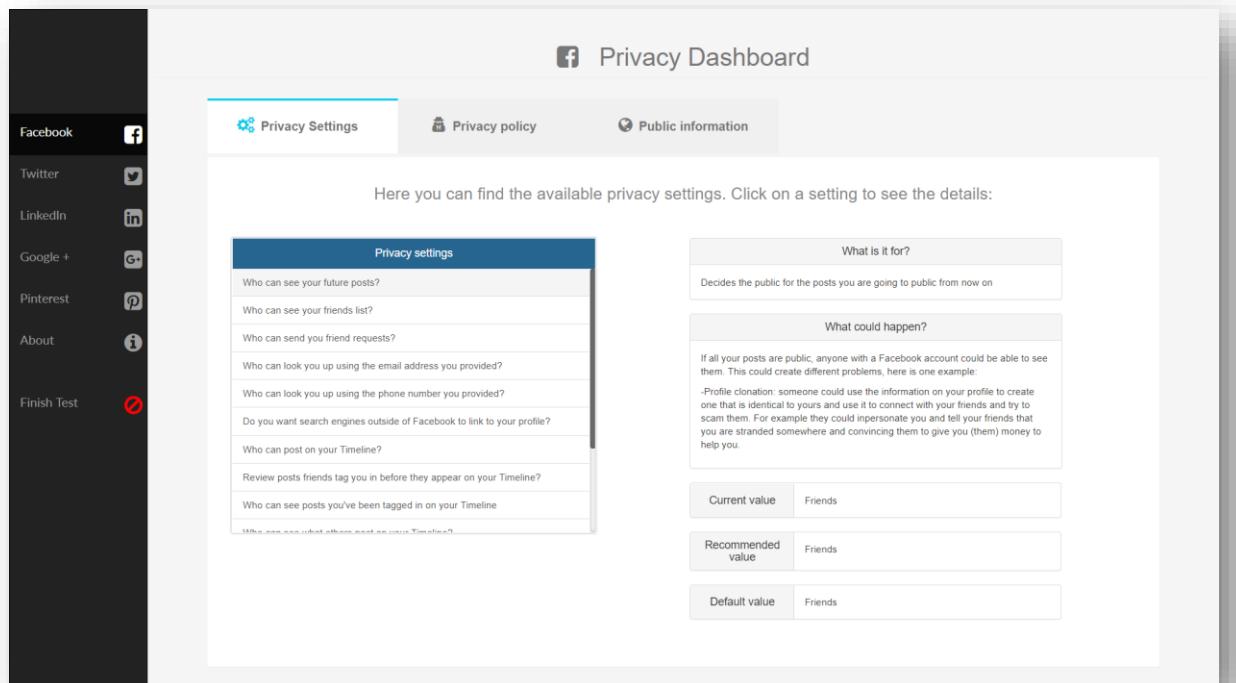
The user should click on “Finish Test” on the left to close the tab and go back to the wizard. This step is not evaluated since it is not really part of the application.

F

Prototype screens

Below are the screenshots of the different screens of the three interfaces of the Privacy Dashboard, used for the usability tests.

Interface 1 - tabs



Privacy Dashboard

Facebook Twitter LinkedIn Google+ Pinterest About Finish Test

Privacy Settings Privacy policy Public information

The Privacy Policy is that document that everyone agrees to without reading when creating an account. Here are the main points:

What info do they collect?	What can they do with it?	Who can they share it with?
Things you do and information you provide.	Provide, improve and develop Services.	People you share and communicate with.
Things others do and information they provide.	Communicate with you.	People that see content others share about you.
Your networks and connections.	Show and measure ads and services.	Apps, websites and third-party integrations on or using our Services.
Information about payments.	Promote safety and security.	Facebook companies.
Device information.		New owner (if changes)
Information from websites and apps that use our Services		Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only)
Information from third-party partners.		Vendors, service providers and other partners.

Privacy Dashboard

Facebook Twitter LinkedIn Google+ Pinterest About Finish Test

Privacy Settings Privacy policy Public information

How private is your profile?

Warning! Your profile is only 20% private

Everything public Still pretty public Almost there Very private

Check below to see what information is visible to anyone on Facebook

Public profile information	Public Photos	Public Posts
 Jack Smith <ul style="list-style-type: none"> Email: thejack@gmail.com Phone Number: 078 362 88 47 Works Groupe e Address: Bvd. de pérolles 28 Relationship status: single Last location tag: was at ancienne gare 3 minutes 	Public Photos 	Public Posts <ul style="list-style-type: none"> Jack 1 month ago such a nice day to go out in the sun Jack 2 months ago not gonna be home for the next two weeks, se you people! Jack 5 months ago I hate my boss! I hope he gets fired soon!

How private is your profile?

Warning! Your profile is only 20% private

Check below to see what information is visible to anyone on Facebook

Public profile information

Jack Smith

- Email: thejack@gmail.com
- Phone Number: 078 362 86 47
- Works Groupe e
- Address: Bvd. de Pérolles 28
- Relationship status: single
- Last location tag: was at ancienne gare 3 minutes ago

Public Photos

Public Posts

- Jack 1 month ago such a nice day to go out in the sun
- Jack 2 months ago not gonna be home for the next two weeks, se you people!
- Jack 5 months ago I hate my boss! I hope he gets fired soon!

SOCIAL NETWORKS PRIVACY DASHBOARD

A DASHBOARD PROTOTYPE TO MANAGE ALL YOUR PRIVACY ON SOCIAL NETWORKS

SCOPE

The scope of this dashboard prototype is to show different design ideas for an application to manage all the aspects of a person's social networks privacy settings

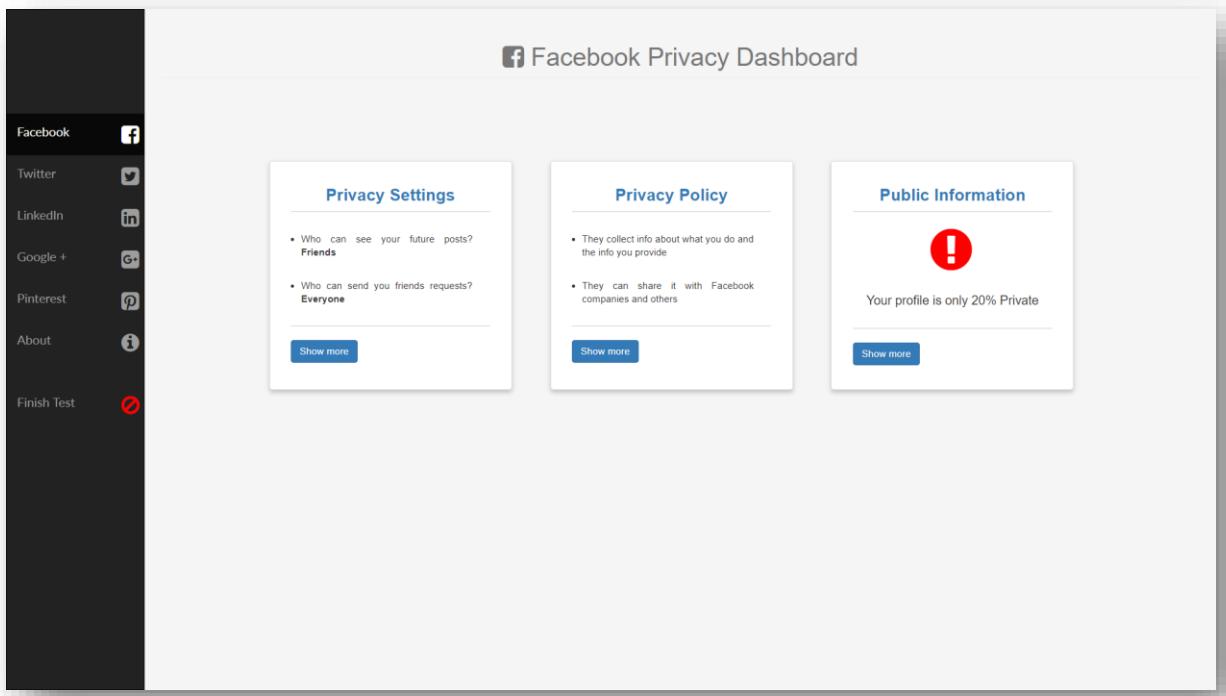
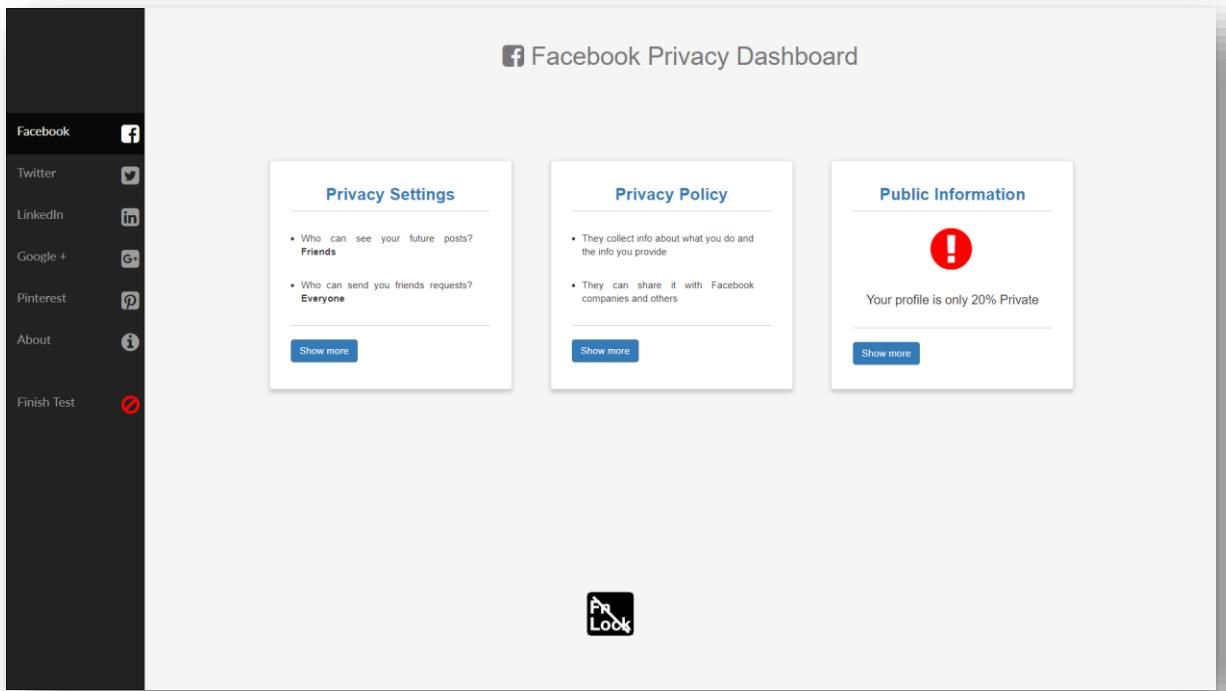
AUTHOR

Angelo Guglielmetti
Information Management
Fribourg University

CONTEXT

The development of this prototype is part of the master thesis I'm writing at the Fribourg university

Interface 2 – tiles



Here is a list of the available privacy settings. Click on a setting to show the details

Privacy settings

- Who can see your future posts?
- Who can see your friends list?
- Who can send you friend requests?
- Who can look you up using the email address you provided?
- Who can look you up using the phone number you provided?
- Do you want search engines outside of Facebook to link to your profile?
- Who can post on your Timeline?
- Review posts friends tag you in before they appear on your Timeline?
- Who can see posts you've been tagged in on your Timeline?

What is it for?

Decides the public for the posts you are going to public from now on

What could happen?

If all your posts are public, anyone with a Facebook account could be able to see them. This could create different problems, here is one example -Profile cloning: someone could use the information on your profile to create one that is identical to yours and use it to connect with your friends and try to scam them. For example they could impersonate you and tell your friends that you are stranded somewhere and convincing them to give you (them) money to help you.

Current value	Friends
Recommended value	Friends
Default value	Friends

The privacy policy is that document that most people agree to without reading it. Here are the main points:

What info do they collect?

- Things you do and information you provide.
- Things others do and information they provide.
- Your networks and connections.
- Information about payments.
- Device information.
- Information from websites and apps that use our Services.
- Information from third-party partners.

What can they do with it?

- Provide, improve and develop Services.
- Communicate with you.
- Show and measure ads and services.
- Promote safety and security.

Who can they share it with?

- People you share and communicate with.
- People that see content others share about you.
- Apps, websites and third-party integrations on or using our Services.
- Facebook companies.
- New owner (if changes)
- Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).
- Vendors, service providers and other partners.

The screenshot shows a user interface for checking privacy settings across various social media platforms. On the left, a sidebar lists platforms: Facebook (selected), Twitter, LinkedIn, Google+, Pinterest, About, and Finish Test. The main area displays a summary for Facebook, indicating a 20% private profile. It includes a slider for adjusting privacy settings from 'Everything public' to 'Very private'. Below this, a message encourages users to check what information is visible to anyone on Facebook. The summary is divided into three sections: 'Public profile information', 'Public Photos', and 'Public Posts'.

Public profile information
Jack Smith

- Email: thejack@gmail.com
- Phone Number: 078 362 88 47
- Works Groupe e
- Address: Bvd. de pérolles 28
- Relationship status: single
- Last location tag: was at ancienne gare 3 minutes ago

Public Photos
A grid of six thumbnail images showing various photos of people and landscapes.

Public Posts
A list of posts by user 'Jack':

- 1 month ago: such a nice day to go out in the sun
- 2 months ago: not gonna be home for the next two weeks, se you people!
- 5 months ago: I hate my boss! I hope he gets fired soon!

Close

Interface 3- Columns

The screenshot shows a dark-themed user interface for 'Privacy Settings'. On the left is a sidebar with a navigation menu:

- Privacy Policy
- Public information
- About
- Finish Test

The main content area is titled 'Privacy settings' and contains the following text:

Here is a list of the available privacy settings on different social networks. Choose up to 3 social networks to see and compare their settings. Click on a single setting to see its details

Below this text are three dropdown menus labeled 'Choose social network'.

This screenshot shows the same interface as above, but with more detailed content displayed in the columns. The sidebar remains the same. The main content area is titled 'Privacy settings' and contains the same introductory text.

The first column displays privacy settings for Facebook:

- Who can see your future posts? (Current state: Friends)
- Who can see your friends list? (Current state: Public)
- Who can send you friend requests? (Current state: Everyone)
- Who can look you up using the email address you provided? (Current state: Everyone)
- Who can look you up using the phone number you provided? (Current state: Everyone)
- Do you want search engines outside of Facebook to link to your profile? (Current state: Yes)
- Who can post on your Timeline?

The second column displays privacy settings for LinkedIn:

- Who can see your connections (Current state: your connections)
- Viewers of this profile also viewed
- Sharing profile edits (Current state: Yes)
- Profile viewing options (Current state: Full Profile)
- Notifying connections when you're in the news (Current state: Yes)
- Who can see your last name
- Followers (Current state: Full)
- Who can post on your Timeline? (Current state: Your Connections)

The third column is a 'Choose social network' dropdown menu with the following options:

- None
- Facebook
- Twitter
- LinkedIn
- Google +
- Pinterest

The Privacy policy is that document to which most people agree without reading when creating an account.
Choose up to 3 social networks to see and compare their privacy policies' main points

Choose social network ▾ Choose social network ▾ Choose social network ▾

The Privacy policy is that document to which most people agree without reading when creating an account.
Choose up to 3 social networks to see and compare their privacy policies' main points

Choose social network ▾

None
Facebook
Twitter
LinkedIn
Google +
Pinterest

Facebook	LinkedIn
What information do they collect	What information do they collect
What can they do with it	What can they do with it
Who can they share it with?	Who can they share it with?

Provide, improve and develop Services.
Communicate with you.
Show and measure ads and services.
Promote safety and security.

The screenshot shows a user interface for a privacy test. On the left, a sidebar menu includes 'Privacy Settings' (with a gear icon), 'Privacy Policy' (with a briefcase icon), 'Public information' (selected, with a person icon), 'About' (with an info icon), and 'Finish Test' (with a red circle icon). The main content area is titled 'Public Information' and contains three sections for different social networks:

- Facebook:** Shows a red exclamation mark icon. Below it, a message says "Warning! Your profile is 20% private" with a progress bar showing 20%. A note below says "Check below to see what information is visible to anyone with an account". Below the note is a "Public Information" card for "Jack Smith" showing a profile picture and a list of details:
 - Email: thejack@gmail.com
 - Phone Number: 078 362 86 47
 - Works Groupe e
 - Adress: Bvd. de périlles 28
 - Relationship status: single
- Twitter:** Shows a yellow exclamation mark icon. Below it, a message says "Your profile is 50% private" with a progress bar showing 50%. A note below says "Check below to see what information is visible to anyone with an account". Below the note is a "Public Information" card for "Public Photos" showing a grid of four thumbnail images.
- Pinterest:** Shows a green checkmark icon. Below it, a message says "Good! Your profile is 100% private" with a progress bar showing 100%. A note below says "Check below to see what information is visible to anyone with an account". Below the note is a "Public Information" card for "Public Photos" showing a grid of four thumbnail images.

G

Prototype test results

Below is the SPSS output of the analyses performed on the results of the usability tests and the corresponding questionnaires.

Starting questionnaire

Age

u-10	0	0.0%
11-20	0	0.0%
21-30	14	77.8%
31-40	3	16.7%
41-50	0	0.0%
51-60	1	5.6%

Gender

Column N %		
Gender	F	33.3%
	M	66.7%

How concerned do you consider yourself about your privacy on social networks, on a scale from 1 (I don't care) to 5 (I care a lot)?

Mean	4.00
Standard Error of Mean	.16
Median	4.00
Maximum	5.00
Minimum	3.00

In my opinion, a social network's privacy policy defines

What information the other social network users can see about me	5	27.8%
What information the social network can collect about me and what they do with it	13	72.2%
I don't know	0	0.0%

How often do you use/visit the following social networks?

	Hourly	Daily	Weekly	Monthly	Less often	I don't have an account
Facebook	38.9%	44.4%	5.6%	0.0%	11.1%	0.0%
Twitter	0.0%	16.7%	0.0%	0.0%	22.2%	61.1%
Linkedin	0.0%	5.6%	11.1%	16.7%	5.6%	61.1%
Google+	0.0%	0.0%	5.6%	5.6%	44.4%	44.4%
Pinterest	0.0%	5.6%	5.6%	0.0%	11.1%	77.8%

How often do you POST something on the following social networks?

	Hourly	Daily	Weekly	Monthly	Less often	I don't have an account
Facebook	0.0%	5.6%	33.3%	33.3%	27.8%	0.0%
Twitter	0.0%	0.0%	11.1%	0.0%	22.2%	66.7%
Linkedin	0.0%	0.0%	0.0%	0.0%	44.4%	55.6%
Google+	0.0%	0.0%	0.0%	0.0%	55.6%	44.4%
Pinterest	0.0%	0.0%	5.6%	5.6%	11.1%	77.8%

When was the last time you checked your privacy settings?

	Last week	Last month	Last year	When creating the account	Never
Facebook	5.6%	38.9%	38.9%	5.6%	11.1%
Twitter	5.6%	5.6%	0.0%	16.7%	72.2%
Linkedin	0.0%	5.6%	11.1%	11.1%	72.2%
Google+	0.0%	5.6%	5.6%	27.8%	61.1%

Pinterest	5.6%	0.0%	0.0%	16.7%	77.8%
-----------	------	------	------	-------	-------

Time to complete the set of tasks per interface

Descriptive Statistics

	Mean	Std. Deviation	N
Total_time_tabs	05:49.94	03:09.18	18
Total_time_tiles	06:45.78	03:23.38	18
Total_time_columns	06:16.89	04:52.98	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser		Huynh-Feldt	Lower-bound	Epsilon ^b
					Greenhouse-Geisser	Huynh-Feldt			Epsilon ^b
Time_interface	.939	1.011	2	.603	.942	1.000		.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: Time_interface

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of Squares						
		df	Mean Square	F	Sig.	Partial Eta Squared	
Time_interface	Sphericity Assumed	28067.593	2	14033.796	.902	.415	.050
	Greenhouse-Geisser	28067.593	1.885	14893.090	.902	.410	.050
	Huynh-Feldt	28067.593	2.000	14033.796	.902	.415	.050
	Lower-bound	28067.593	1.000	28067.593	.902	.356	.050
Error(Time_interface)	Sphericity Assumed	528949.074	34	15557.326			
	Greenhouse-Geisser	528949.074	32.038	16509.906			
	Huynh-Feldt	528949.074	34.000	15557.326			
	Lower-bound	528949.074	17.000	31114.651			

Percentage of successfully completed tasks per interface

Descriptive Statistics

	Mean	Std. Deviation	N
Percent_correct_tabs	.7639	.20262	18
Percent_correct_tiles	.7176	.21416	18
Percent_correct_columns	.7778	.20809	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b Lower-bound
error_perc	.934	1.094	2	.579	.938	1.000	.500

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: error_perc

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
error_perc	Sphericity Assumed	.036	2	.018	.728	.490	.041
	Greenhouse-Geisser	.036	1.876	.019	.728	.482	.041
	Huynh-Feldt	.036	2.000	.018	.728	.490	.041
	Lower-bound	.036	1.000	.036	.728	.405	.041
Error(error_perc)	Sphericity Assumed	.835	34	.025			

Greenhouse-Geisser	.835	31.892	.026			
Huynh-Feldt	.835	34.000	.025			
Lower-bound	.835	17.000	.049			

Percentage of successfully completed tasks depending on chronological position

Descriptive Statistics

	Mean	Std. Deviation	N
Percent_correct_first	.6528	.22370	18
Percent_correct_second	.7870	.19642	18
Percent_correct_third	.8194	.16482	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
learn_task	.988	.199	2	.905	.988	1.000	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: learn_task

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
learn_task	Sphericity Assumed	.281	2	.141	8.110	.001	.323
	Greenhouse-Geisser	.281	1.976	.142	8.110	.001	.323
	Huynh-Feldt	.281	2.000	.141	8.110	.001	.323
	Lower-bound	.281	1.000	.281	8.110	.011	.323
Error(learn_task)	Sphericity Assumed	.589	34	.017			
	Greenhouse-Geisser	.589	33.585	.018			
	Huynh-Feldt	.589	34.000	.017			
	Lower-bound	.589	17.000	.035			

Pairwise Comparisons

(I) learn_task	(J) learn_task	(I-J)	95% Confidence Interval for Difference ^b				
			Mean Difference	Std. Error	Sig. ^b	Lower Bound	Upper Bound
1	2	-.134*	.042	.016		-.246	-.022
	3	-.167*	.046	.007		-.289	-.044

2	1	.134*	.042	.016	.022	.246
	3	-.032	.043	1.000	-.147	.082
3	1	.167*	.046	.007	.044	.289
	2	.032	.043	1.000	-.082	.147

Based on estimated marginal means

*. The mean difference is significant at the .05 level. b. Adjustment for multiple comparisons: Bonferroni.

Time to complete task set depending on chronological position

Descriptive Statistics

	Mean	Std. Deviation	N
Time_total_first	07:31	04:49	18
Time_total_second	05:50	03:05	18
Time_total_third	05:31	03:14	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
learn_time	.922	1.296	2	.523	.928	1.000	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: learn_time

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
learn_time	Sphericity Assumed	150181.815	2	75090.907	6.275	.005	.270
	Greenhouse-Geisser	150181.815	1.856	80931.597	6.275	.006	.270
	Huynh-Feldt	150181.815	2.000	75090.907	6.275	.005	.270
	Lower-bound	150181.815	1.000	150181.815	6.275	.023	.270
Error(learn_time)	Sphericity Assumed	406834.852	34	11965.731			
	Greenhouse-Geisser	406834.852	31.546	12896.444			
	Huynh-Feldt	406834.852	34.000	11965.731			
	Lower-bound	406834.852	17.000	23931.462			

Pairwise Comparisons

(I) learn_time	(J) learn_time	(I-J)	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
					Lower Bound	Upper Bound
1	2	100.944	41.156	.076	-8.326	210.214
	3	120.278*	34.744	.009	28.034	212.522
2	1	-100.944	41.156	.076	-210.214	8.326
	3	19.333	32.979	1.000	-68.226	106.892
3	1	-120.278*	34.744	.009	-212.522	-28.034
	2	-19.333	32.979	1.000	-106.892	68.226

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Time to finish the “Privacy settings” tasks

Within-Subjects Factors

time_settings	Dependent Variable
1	tabs_time_settings
2	tiles_time_settings
3	columns_time_settings

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_time_settings	237.0556	201.05968	18
tiles_time_settings	155.6667	102.71205	18
columns_time_settings	164.2222	190.45041	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
time_settings	.345	17.044	2	.000	.604	.625	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: time_settings

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
time_settings	Sphericity Assumed	72012.259	2	36006.130	1.735	.192	.093
	Greenhouse-Geisser	72012.259	1.208	59602.792	1.735	.204	.093
	Huynh-Feldt	72012.259	1.251	57586.751	1.735	.204	.093
	Lower-bound	72012.259	1.000	72012.259	1.735	.205	.093
Error(time_settings)	Sphericity Assumed	705521.074	34	20750.620			
	Greenhouse-Geisser	705521.074	20.539	34349.565			
	Huynh-Feldt	705521.074	21.259	33187.704			
	Lower-bound	705521.074	17.000	41501.240			

Pairwise Comparisons

(I) time_settings	(J) time_settings	(I-J)	95% Confidence Interval for Difference ^a			
			Mean Difference	Std. Error	Sig. ^a	Lower Bound
1	2	81.389	49.743	.361	.361	-50.679
	3	72.833	61.896	.767	.767	-91.499
2	1	-81.389	49.743	.361	.361	-213.457
	3	-8.556	24.727	1.000	1.000	-74.206
3	1	-72.833	61.896	.767	.767	-237.166
	2	8.556	24.727	1.000	1.000	-57.095

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Time to finish the “Comparison” tasks

Within-Subjects Factors

time_comparison	Dependent
	Variable
1	tabs_time_comp arison
2	tiles_time_comp arison
3	columns_time_c omparison

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_time_comparison	104.6667	63.47487	18
tiles_time_comparison	55.1111	23.29577	18
columns_time_comparison	72.5000	42.32264	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b Lower-bound
time_comparison	.886	1.941	2	.379	.897	.997	.500

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: time_comparison

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of Squares		df	Mean Square	F	Sig.	Partial Eta Squared
time_comparison	Sphericity Assumed	22756.926	2	11378.463	7.921	.001	.318
	Greenhouse-Geisser	22756.926	1.795	12678.153	7.921	.002	.318
	Huynh-Feldt	22756.926	1.993	11416.216	7.921	.002	.318
	Lower-bound	22756.926	1.000	22756.926	7.921	.012	.318
Error(time_comparison)	Sphericity Assumed	48841.741	34	1436.522			
	Greenhouse-Geisser	48841.741	30.515	1600.607			
	Huynh-Feldt	48841.741	33.888	1441.288			
	Lower-bound	48841.741	17.000	2873.044			

Pairwise Comparisons

(I) time_comparison	(J) time_comparison	Mean Difference		Sig. ^b	95% Confidence Interval for Difference ^b	
		(I-J)	Std. Error		Lower Bound	Upper Bound
1	2	49.556*	14.582	.010	10.842	88.270
	3	32.167*	11.907	.045	.554	63.779
2	1	-49.556*	14.582	.010	-88.270	-10.842
	3	-17.389	11.156	.412	-47.007	12.229
3	1	-32.167*	11.907	.045	-63.779	-.554
	2	17.389	11.156	.412	-12.229	47.007

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Time to finish “Privacy policy” tasks

Within-Subjects Factors

time_policy	Dependent Variable
1	tabs_time_policy
2	tiles_time_policy
3	columns_time_policy

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_time_policy	57.3333	60.17230	18
tiles_time_policy	99.1111	58.86264	18
columns_time_policy	80.2778	43.69521	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon ^b		
					Greenhouse-Geisser	Huynh-Feldt	Lower-bound
time_policy	.657	6.723	2	.035	.745	.800	.500

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: time_policy

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
time_policy	Sphericity Assumed	15759.148	2	7879.574	4.072	.026	.193
	Greenhouse-Geisser	15759.148	1.489	10582.717	4.072	.040	.193
	Huynh-Feldt	15759.148	1.599	9854.572	4.072	.036	.193
	Lower-bound	15759.148	1.000	15759.148	4.072	.060	.193
Error(time_policy)	Sphericity Assumed	65793.519	34	1935.103			
	Greenhouse-Geisser	65793.519	25.315	2598.954			
	Huynh-Feldt	65793.519	27.186	2420.133			
	Lower-bound	65793.519	17.000	3870.207			

Pairwise Comparisons

(I) time_policy	(J) time_policy	(I-J)	Mean Difference	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
						Lower Bound	Upper Bound
1	2	-41.778*	10.087	.002		-68.559	-14.997
	3	-22.944	14.965	.431		-62.678	16.789
2	1	41.778*	10.087	.002		14.997	68.559
	3	18.833	17.870	.920		-28.610	66.277
3	1	22.944	14.965	.431		-16.789	62.678
	2	-18.833	17.870	.920		-66.277	28.610

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Time to finish “Public information” tasks

Within-Subjects Factors

Dependent

time_public2	Variable
1	tabs_time_public
2	tiles_time_public
3	columns_time_public

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_time_public	64.8333	52.36776	18
tiles_time_public	95.8889	95.55651	18
columns_time_public	59.8889	72.97291	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
time_public2	.592	8.383	2	.015	.710	.756	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: time_public2

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of Squares						Sig.	Partial Eta Squared
		df	Mean Square	F				
time_public2	Sphericity Assumed	13709.370	2	6854.685	1.595	.218		.086
	Greenhouse-Geisser	13709.370	1.421	9650.252	1.595	.224		
	Huynh-Feldt	13709.370	1.513	9061.198	1.595	.223		
	Lower-bound	13709.370	1.000	13709.370	1.595	.224		
Error(time_public2)	Sphericity Assumed	146098.630	34	4297.019				
	Greenhouse-Geisser	146098.630	24.151	6049.485				
	Huynh-Feldt	146098.630	25.721	5680.223				
	Lower-bound	146098.630	17.000	8594.037				

Pairwise Comparisons

(I) time_public2	(J) time_public2	(I-J)	Mean Difference	95% Confidence Interval for		
				Std. Error	Sig. ^a	Difference ^a
1	2	-31.056	21.761	.515	-88.830	26.718
	3	4.944	14.676	1.000	-34.019	43.908
2	1	31.056	21.761	.515	-26.718	88.830
	3	36.000	27.266	.613	-36.392	108.392
3	1	-4.944	14.676	1.000	-43.908	34.019
	2	-36.000	27.266	.613	-108.392	36.392

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Percentage of successfully completed “Privacy settings” tasks

Within-Subjects Factors

corr_settings	Dependent Variable
1	tabs_corr_settings
2	tiles_corr_settings
3	columns_corr_settings

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_corr_settings	2.6111	.58298	18
tiles_corr_settings	2.4722	.62948	18
columns_corr_settings	2.7500	.42875	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon ^b		
					Greenhouse-Geisser	Huynh-Feldt	Lower-bound
corr_settings	.814	3.287	2	.193	.843	.926	.500

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: corr_settings

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of					
	Squares	df	Mean Square	F	Sig.	Partial Eta Squared
corr_settings	Sphericity Assumed	.694	2	.347	1.341	.275
	Greenhouse-Geisser	.694	1.687	.412	1.341	.274
	Huynh-Feldt	.694	1.852	.375	1.341	.275
	Lower-bound	.694	1.000	.694	1.341	.263
Error(corr_settings)	Sphericity Assumed	8.806	34	.259		
	Greenhouse-Geisser	8.806	28.675	.307		
	Huynh-Feldt	8.806	31.486	.280		
	Lower-bound	8.806	17.000	.518		

Pairwise Comparisons

(I) corr_settings	(J) corr_settings	(I-J)	Std. Error	Sig. ^a	95% Confidence Interval for Difference ^a	
					Mean Difference	Lower Bound
1	2	.139	.193	1.000	-.374	.651
	3	-.139	.180	1.000	-.617	.339
2	1	-.139	.193	1.000	-.651	.374
	3	-.278	.129	.139	-.621	.065
3	1	.139	.180	1.000	-.339	.617
	2	.278	.129	.139	-.065	.621

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Percentage of successfully completed “Comparison” tasks

Within-Subjects Factors

corr_comparison	Dependent Variable
1	tabs_corr_comparison
2	tiles_corr_comparison
3	columns_corr_comparison

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_corr_comparison	.5833	.46177	18
tiles_corr_comparison	.8611	.28726	18
columns_corr_comparison	.6944	.38877	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
corr_comparison	.980	.327	2	.849	.980	1.000	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: corr_comparison

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
		Squares					
corr_comparison	Sphericity Assumed	.704	2	.352	2.584	.090	.132
	Greenhouse-Geisser	.704	1.960	.359	2.584	.091	.132
	Huynh-Feldt	.704	2.000	.352	2.584	.090	.132
	Lower-bound	.704	1.000	.704	2.584	.126	.132
Error(corr_comparison)	Sphericity Assumed	4.630	34	.136			
	Greenhouse-Geisser	4.630	33.326	.139			
	Huynh-Feldt	4.630	34.000	.136			
	Lower-bound	4.630	17.000	.272			

Pairwise Comparisons

(I) corr_comparison	(J) corr_comparison	(I-J)	Mean Difference		95% Confidence Interval for Difference ^a		
			Std. Error	Sig. ^a	Lower Bound	Upper Bound	
1	2	-.278	.129	.139	-.621	.065	
	3	-.111	.125	1.000	-.443	.221	
2	1	.278	.129	.139	-.065	.621	
	3	.167	.114	.489	-.137	.470	
3	1	.111	.125	1.000	-.221	.443	
	2	-.167	.114	.489	-.470	.137	

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Percentage of successfully completed “Privacy policy” tasks

Within-Subjects Factors

corr_policy	Dependent Variable
1	tabs_corr_policy
2	tiles_corr_policy
3	columns_corr_policy

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_corr_policy	.7778	.42779	18
tiles_corr_policy	.4722	.46880	18
columns_corr_policy	.5278	.49918	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
corr_policy	.705	5.594	2	.061	.772	.835	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: corr_policy

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of Squares						Sig.	Partial Eta Squared
		df	Mean Square	F				
corr_policy	Sphericity Assumed	.954	2	.477	2.415	.105		.124
	Greenhouse-Geisser	.954	1.544	.618	2.415	.120		.124
	Huynh-Feldt	.954	1.669	.571	2.415	.115		.124
	Lower-bound	.954	1.000	.954	2.415	.139		.124
Error(corr_policy)	Sphericity Assumed	6.713	34	.197				
	Greenhouse-Geisser	6.713	26.254	.256				
	Huynh-Feldt	6.713	28.376	.237				
	Lower-bound	6.713	17.000	.395				

Pairwise Comparisons

(I) corr_policy	(J) corr_policy	(I-J)	95% Confidence Interval for Difference ^a				
			Mean Difference	Std. Error	Sig. ^a	Lower Bound	Upper Bound
1	2	.306	.172	.281		-.152	.763
	3	.250	.101	.073		-.018	.518
2	1	-.306	.172	.281		-.763	.152
	3	-.056	.161	1.000		-.483	.372
3	1	-.250	.101	.073		-.518	.018
	2	.056	.161	1.000		-.372	.483

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Percentage of successfully completed “Public information” tasks

Within-Subjects Factors

time_public Dependent Variable	
1	tabs_corr_public
2	tiles_corr_public
3	columns_corr_public

Descriptive Statistics

	Mean	Std. Deviation	N
tabs_corr_public	.6111	.47140	18
tiles_corr_public	.5000	.51450	18
columns_corr_public	.6944	.45822	18

Mauchly's Test of Sphericity^a

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon ^b		
					Greenhouse-Geisser	Huynh-Feldt	Lower-bound
time_public	.905	1.590	2	.452	.914	1.000	.500

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: time_public

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Source	Type III Sum of		df	Mean Square	F	Sig.	Partial Eta Squared
	Squares						
time_public	Sphericity Assumed	.343	2	.171	1.129	.335	.062
	Greenhouse-Geisser	.343	1.827	.187	1.129	.332	.062
	Huynh-Feldt	.343	2.000	.171	1.129	.335	.062
	Lower-bound	.343	1.000	.343	1.129	.303	.062
Error(time_public)	Sphericity Assumed	5.157	34	.152			
	Greenhouse-Geisser	5.157	31.062	.166			
	Huynh-Feldt	5.157	34.000	.152			
	Lower-bound	5.157	17.000	.303			

Pairwise Comparisons

(I) time_public	(J) time_public	(I-J)	Std. Error	Sig. ^a	95% Confidence Interval for Difference ^a	
					Lower Bound	Upper Bound
1	2	.111	.143	1.000	-.269	.491
	3	-.083	.109	1.000	-.372	.206
2	1	-.111	.143	1.000	-.491	.269
	3	-.194	.135	.503	-.553	.164
3	1	.083	.109	1.000	-.206	.372
	2	.194	.135	.503	-.164	.553

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Ease of use evaluation of the single interfaces

Frequencies

		Count	Column N %
Columns	very difficult	0	0.0%
	difficult	3	16.7%
	average	7	38.9%
	easy	4	22.2%
	very easy	4	22.2%
Tiles	very difficult	1	5.6%
	difficult	2	11.1%
	average	9	50.0%
	easy	6	33.3%
	very easy	0	0.0%
Tabs	very difficult	0	0.0%
	difficult	1	5.6%
	average	12	66.7%
	easy	5	27.8%
	very easy	0	0.0%

Within-Subjects Factors

Dependent

ease_of_use	Variable
1	Ease_Tabs
2	Ease_Tiles
3	Ease_Columns

Descriptive Statistics

	Mean	Std. Deviation	N
Ease_Tabs	3.2222	.54832	18
Ease_Tiles	3.1111	.83235	18
Ease_columns	3.5000	1.04319	18

Mauchly's Test of Sphericity^a

Measure: MEASURE_1

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
ease_of_use	.984	.253	2	.881	.985	1.000	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: ease_of_use

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Measure: MEASURE_1

Source	Type III Sum of		df	Mean Square	F	Sig.
	Squares					
ease_of_use	Sphericity Assumed	1.444	2	.722	1.277	.292
	Greenhouse-Geisser	1.444	1.969	.734	1.277	.292
	Huynh-Feldt	1.444	2.000	.722	1.277	.292
	Lower-bound	1.444	1.000	1.444	1.277	.274
Error(ease_of_use)	Sphericity Assumed	19.222	34	.565		
	Greenhouse-Geisser	19.222	33.475	.574		
	Huynh-Feldt	19.222	34.000	.565		
	Lower-bound	19.222	17.000	1.131		

Ease of comparison evaluation for the single interfaces

Frequencies

	Count	Column N %
Columns	very difficult	0 0.0%
	difficult	2 11.1%
	average	5 27.8%
	easy	6 33.3%
	very easy	5 27.8%
Tiles	very difficult	1 5.6%
	difficult	2 11.1%
	average	6 33.3%
	easy	8 44.4%
	very easy	1 5.6%
Tabs	very difficult	0 0.0%
	difficult	3 16.7%
	average	8 44.4%
	easy	6 33.3%
	very easy	1 5.6%

Within-Subjects Factors

Measure: MEASURE_1

ease_compare	Dependent Variable
1	Ease_comparison_Tabs
2	Ease_comparison_Tiles
3	Ease_comparison_columns

Descriptive Statistics

	Mean	Std. Deviation	N
Ease_comparison_Tabs	3.2778	.82644	18
Ease_comparison_Tiles	3.3333	.97014	18
Ease_comparison_Columns	3.7778	1.00326	18

Mauchly's Test of Sphericity^a

Measure: MEASURE_1

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Greenhouse-Geisser	Huynh-Feldt	Epsilon ^b	Lower-bound
ease_compare	.897	1.733	2	.420	.907	1.000	.500	

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a. Design: Intercept

Within Subjects Design: ease_compare

b. May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

Tests of Within-Subjects Effects

Measure: MEASURE_1

Source	Type III Sum of		df	Mean Square	F	Sig.
	Squares					
ease_compare	Sphericity Assumed	2.704	2	1.352	2.657	.085
	Greenhouse-Geisser	2.704	1.814	1.491	2.657	.091
	Huynh-Feldt	2.704	2.000	1.352	2.657	.085
	Lower-bound	2.704	1.000	2.704	2.657	.121
Error(ease_compare)	Sphericity Assumed	17.296	34	.509		
	Greenhouse-Geisser	17.296	30.834	.561		
	Huynh-Feldt	17.296	34.000	.509		
	Lower-bound	17.296	17.000	1.017		

Final questionnaire

Interface preference

Interface	Percentage
tabs	38.9%
tiles	27.8%
columns	33.3%

Final questions

	strongly disagree	disagree	neutral	agree	strongly agree
The tool provides useful information about privacy on social networks	0.0%	0.0%	5.6%	38.9%	55.6%
The privacy assessment of the profile was useful	0.0%	0.0%	16.7%	33.3%	50.0%
The tool made me think more about privacy on social networks	0.0%	5.6%	16.7%	50.0%	27.8%
I learned something I didn't know before using this tool	0.0%	11.1%	22.2%	44.4%	22.2%
If it was available, I would use it	5.6%	0.0%	11.1%	55.6%	27.8%

H

Source Code

The source code for the different interfaces as well as for the wizard can be found online in the following repositories, as well as on the attached CD:

Wizard: <https://bitbucket.org/engid87/homepage>

Interface 1 – Tabs: <https://bitbucket.org/engid87/interface-1-tabs>

Interface 2 – Tiles: <https://bitbucket.org/engid87/interface-2-tiles>

Interface 3 – Columns: <https://bitbucket.org/engid87/interface-3-columns>