DATATILSYNET

Social Network Services and Privacy

A case study of Facebook

Atle Årnes, Jørgen Skorstad and Lars-Henrik Paarup Michelsen

15.04.2011

Table of content

0. Executive Summary

The *Norwegian Consumer Council* has asked the Data Inspectorate of Norway to answer a set of questions regarding *Facebook*; for instance about collecting of sensitive data, user consent and disclosure of personal information to third parties. Another topic is whether the Norwegian Personal Data Act applies to the processing of personal data that are carried out within the Facebook system.

Eventually this complaint was one of various factors that led to the formation of a team of officers at the Inspectorate, who have examined the Facebook service, and prepared this report.

Throughout the preparation process, we have made some discoveries that we have found to be quite interesting, naturally some more than others, amongst which are as follows:

- We have discovered that the *Privacy Policy* and *the Statement of Rights and Responsibilities* are quite extensive, and
- that the documents should be read in light of each other
- We have discovered that these documents can give valuable insight into the processing of information that is being carried out within the Facebook system
- Also, we have discovered that sometimes the wording of the clauses can be vague and difficult to understand, at least when it comes to the sections regarding
    - the processing of the user's *IP addresses*
    - the *tracking of web pages* that users "see"
    - the scope of the policy

In other words, we also found there was a certain lack of transparency.

- We have experienced how adding information to the personal profile leads to more customised advertisements
- We have pointed out that the use of social plug-ins can generate vast amounts of data about Facebook's users, both when they are logged onto Facebook and when they are not, and in our point of view this is particularly interesting in light of the fact that Facebook collects the users' IP addresses
- It seems that *information* about some non users are also collected, namely through
    - the Friend Finder
    - social plug-ins
- How to delete an account or personal information
- We have drawn up two different approaches to the problem of jurisdiction
- We have found out that other authorities have collaborated successfully with Facebook, in order to heighten the standards of the protection of Facebook users' personal data

The Data Inspectorate of Norway considers that it has an obligation to contribute to raising awareness about the privacy aspects of using social networking services such as Facebook.

It is also the Data Inspectorate's intention to address some of these issues directly to Facebook. Consequently this report will be sent to both the office in Ireland and the USA. A formal handling of the complaint from the Consumer Council will ensue shortly. The Inspectorate will continue to follow the developments in the Social Network Services sector with great interest.

1. Introduction

On October 18th 2010 *The Norwegian Data Inspectorate* appointed a team to write a preliminary report on "Facebook and Social Media", due to a complaint filed earlier this year by *the Consumer Council of Norway* about Facebook.[1] The Council argues that that the company violates *The Norwegian Personal Data Act* ("The Act") [2] on several grounds.

Furthermore *The Data Inspectorate* was requested to elaborate more in general on whether and how social networking services and providers of third party applications are allowed to process the personal information on Facebook's users, under the Act.

As Facebook is a vast topic of its own, and considering the fact that this report had to be completed within a relatively short period of time, the team did not, unfortunately, have the opportunity to carry out a more thorough study of social media in general.[3] Instead we have chosen to examine the Privacy Policy of Facebook, and its adhering documents. We have also been interested in the consequences of Facebook's affiliation to third parties, and its use of so-called *social plug-ins*. This examination is far from exhaustive – however, it has been our aim and our hope that a foundation for further research on this fascinating subject can be based on this examination.

Our *modus operandi* can be summarised in the following bullet points:

- *Studying of various texts*
  There is an abundance of written information about Facebook, both from Facebook itself and from other external sources. Early on in the process we decided to focus our attention on Facebook's many documents related to user privacy and its Statements of Rights and Responsibilities. Also, a report on Facebook published by *The Privacy Commissioner of Canada* (2009)[4] has been read with great interest. Reference to the relevant written material is given in footnotes throughout the present document.

- *Meetings with different specialists*
  During the project we have had meetings or correspondence with the following institutions and people:
  - The Norwegian Consumer Ombudsman
  - The Norwegian Consumer Council
  - Gisle Hannemyr, lecturer at the Department of Informatics at the University of Oslo
  - Ole Tom Seierstad, Chief Security Advisor at Microsoft Norway
  - Inger Anne Tøndel and Karin Bernsmed, COPE – Comprehensive Privacy for End users

[1] The complaint also includes the third party application provider Zynga; however this company has not undergone any particular scrutiny in connection with the preparation of this this report. The complaint is found at: http://forbrukerportalen.no/Artikler/2010/Facebook_and_Zynga_reported_to_the_Data_Inspectorate

[2] Act of 14 April 2000 no. 31 relating to the processing of personal data.

[3] The Data Inspectorate did, however, conduct a series of audits of Norwegian social service providers during spring 2010.

[4] http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

    - Dag Wiese Schartum, Professor at Norwegian Research Centre for Computers and Law, the University of Oslo
    - The Data Protection Authority in Hamburg, Germany

- *"Field research"*
  As a part of the project we also made use of one iPhone, one iPad, one Samsung Galaxy Tab (Android) and one Sony Ericsson Phone (Symbian) in order to experience how Facebook and applications work from different platforms.

Writing a report on Facebook is like aiming at a moving target. Not only has there been made changes to Facebook's services and conditions since The Council filed their complaint, there has also been made alterations since we started working on this report – for instance, Facebook Places has in the meantime been made available to Norwegian users. The version of the Privacy Policy that comsitutes the basis for this document, was last updated on October 5th 2010.

We have consciously distinguished between, on the one hand, circumstances which are objectively verifiable, such as the wording of the conditions, and on the other, our own assumptions, such as regarding the circumstances surrounding Facebook's collection of IP-addresses. All this is hopefully reflected in the report's applied terminology, through the use of phrases like "our guess is", "we assume", and similar subjectivities.

On behalf of the Data Inspectorate, we welcome any feedback on this report, whether from Facebook or from anyone else. In doing so, please send your comments to the following e-mail address or postal address:

FB-prosjektet@datatilsynet.no

Datatilsynet
Postboks 8177 Dep.
0034 OSLO
NORWAY

2. About Facebook

In February 2004 Mark Zuckerberg launched a network for students at Harvard University named "The Facebook". In September 2006, Facebook was opened for everyone with a valid e-mail address and eight months later, in May 2007, Facebook also invited third party applications to interact with the increasing number of Facebook users through Facebook Platform.

From 2004 till 2010 the number of Facebook users increased from 1 million till 500 million users. This has made Facebook the dominant social network in the world.

Facts about Facebook

- There are over 900 million objects on Facebook that people interact with (pages, groups, events and community pages)
- Average user is connected to 80 community pages, groups and events
- Average user creates 90 pieces of content each month
- Average user has 130 friends
- More than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month.

Source: *www.facebook.com*

2.1. Facebook's "*appetite*" for personal information

Facebook was created to be a personal network for real people. Unlike other social networks, Facebook does not accept members to register with fake names, nicknames or aliases. Providing incorrect information in the registration process, or creating more than one Facebook profile, is a violation of Facebook's Statement of Rights and Responsibilities.[5]

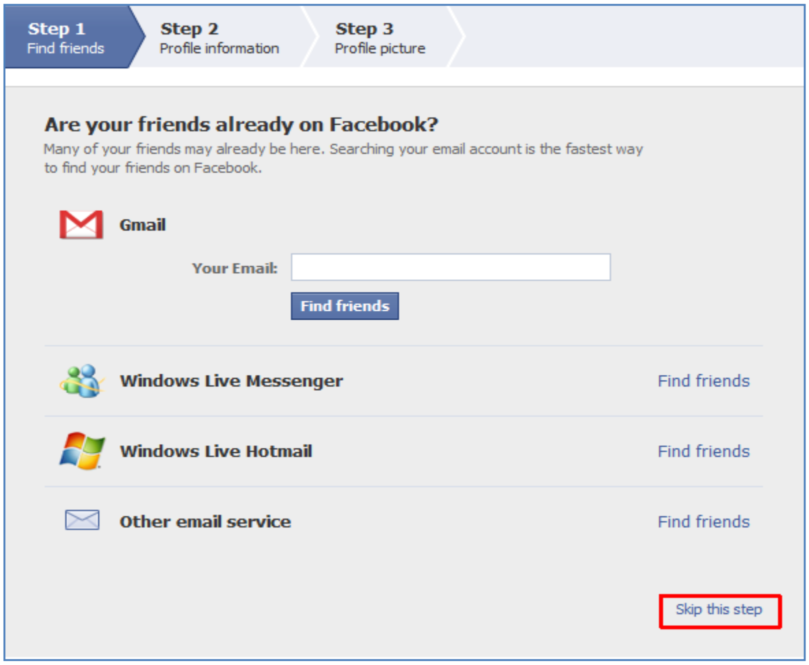
From the age of 13 everyone with Internet access can sign up for a Facebook account. When doing so one must provide the following information, as a minimum:

- Name
- Gender
- E-mail
- Date of birth

These four categories of information are mandatory, and the members of the network can avoid providing Facebook with any more personal information than this. However, our experience from this project is that Facebook will "attempt" to obtain supplementary information from their users. Already during the three-step registration process, Facebook reminds you that you can provide them with further information, such as your *e-mail contacts*, name of *school*, *university or college* and *employer* and a *profile photo*.

This is how the three-step registration process might look like:[6]

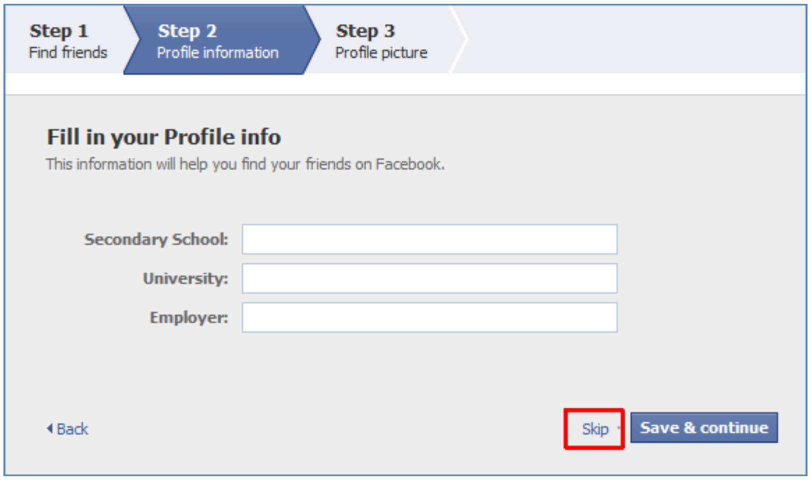
[5] Cf. section 4 of the Statement of Rights and Responsibilities.
[6] We assume that it does each time.



Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

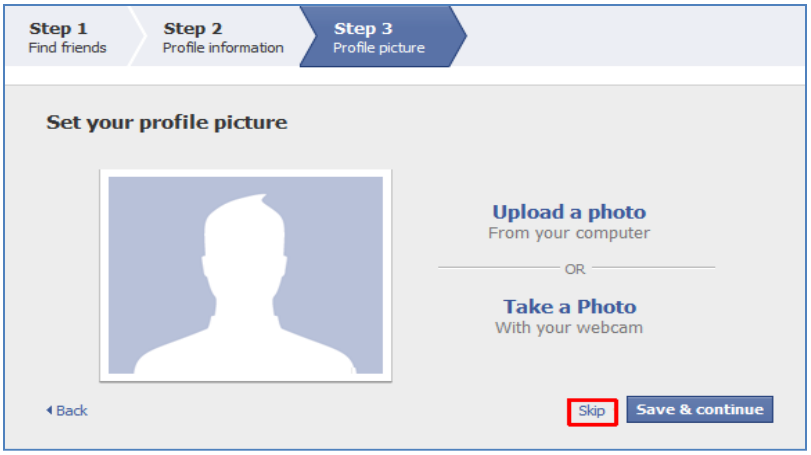
Figure 1: Facebook asks for access to your contact list



Fill in your Profile info

This information will help you find your friends on Facebook.

Figure 2: Facebook asks for the name of your school, university and employer

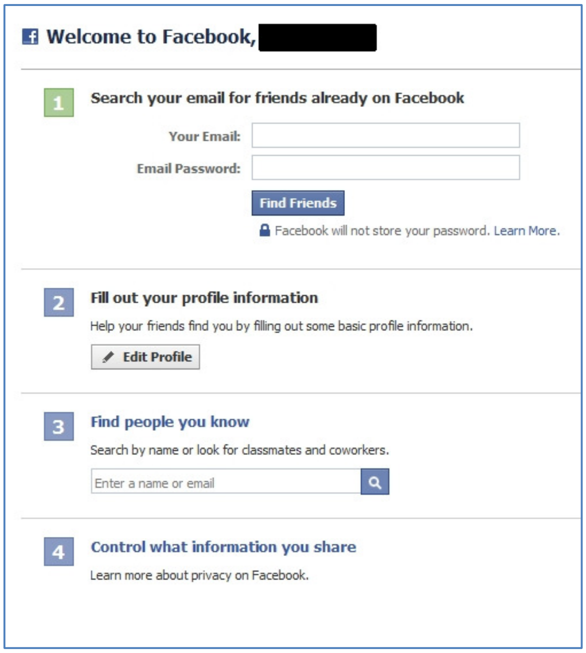


Set your profile picture

Figure 3: Facebook asks you to upload or take a profile photo

When these three steps in the registration process are finished, most people are likely to have provided Facebook with more information than the mandatory categories. If one does not spot the link labelled "*skip*", the user might be inclined to believe that he or she needs to fill out all the inquired information.

Facebook will persist in asking for more personal information, also after the registration process is finished and you have logged off. The next time you log on to Facebook as a member, you are once again asked to further "*Fill out your Profile information*".



Welcome to Facebook, [redacted]

1 Search your email for friends already on Facebook

Your Email:

Email Password:

Find Friends

Facebook will not store your password. Learn More.

2 Fill out your profile information

Help your friends find you by filling out some basic profile information.

Edit Profile

3 Find people you know

Search by name or look for classmates and coworkers.

Enter a name or email

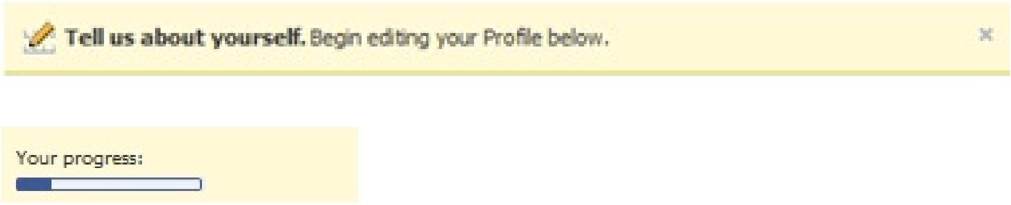
4 Control what information you share

Learn more about privacy on Facebook.

Figure 4: Facebook's reminder

At first we ignored the encouragement from Facebook to provide more personal information. However, when the same message appeared continuously on the profile site, we yielded in the end and added further information about our hometown, political view, religious view, sexual preferences, favourite quotation, and so on.

The next time we logged on to Facebook, the reminder to supply further personal information was now to be found through two banners on our profile site. One banner was saying "Tell us about yourself" and the other indicated by using a graph that our registration process was far from finished.



Tell us about yourself. Begin editing your Profile below.

Your progress:

Figure 5: These banners keep appearing on our profiles

It seems unclear to what extent one has to submit personal information in order to make the reminders disappear. However, it should be noted that at this point we had not yet started using the account actively, in the meaning integrating with other people and objects, sharing digital content, and so on.

2.2. What categories of personal information is being processed?

In order to understand what kind of personal information that Facebook is processing, and the amount of data involved, a reference to Bruce Schneier's essay "*A taxonomy of social networking data*" can be helpful.[7] Based on Schneier's taxonomy, we have divided the personal data processed by Facebook, relating in some way or other to its users, into the following categories:

Category	**Definition**	**Type of data**
Mandatory profile data	Personal data one has to provide in order to be a member	Name, gender, e-mail and date of birth
Extended profile data	Personal data one may provide	Network, profile photo, mobile phone number, hometown, sexual preferences, name of school/university, religious/political views, favourite music/film/author, name of family members, e-mail contacts, etc.
Personal network data	Data showing your interaction with other people and objects on Facebook	Friends list, family, relationships, pages/groups/people you like, etc.
Self published data at home	Data one publishes or uploads on one's own profile	News feeds, notes, photos, videos, links, etc.
Self published data away	Data one publishes on someone others profile	Comments, wall messages, etc.
Other users' data	Data about you published by other users	Photo, video, tags, etc.
Behavioural data	Data Facebook collects about your habits	Pages you visit, topics you write about, games you play, etc.
Connection data	Data from your connection to Facebook	Type of connection unit (mobile or PC), browser, location of connection unit and IP address.
Metadata	Data about data	Type of camera used to take an uploaded photo, etc.
Derived data	Data about you derived from all other data	If 90 percent of your friends from your University network are fan of a special rock band, you are probably a fan too.

Table 1: Ten categories of personal data processed by Facebook

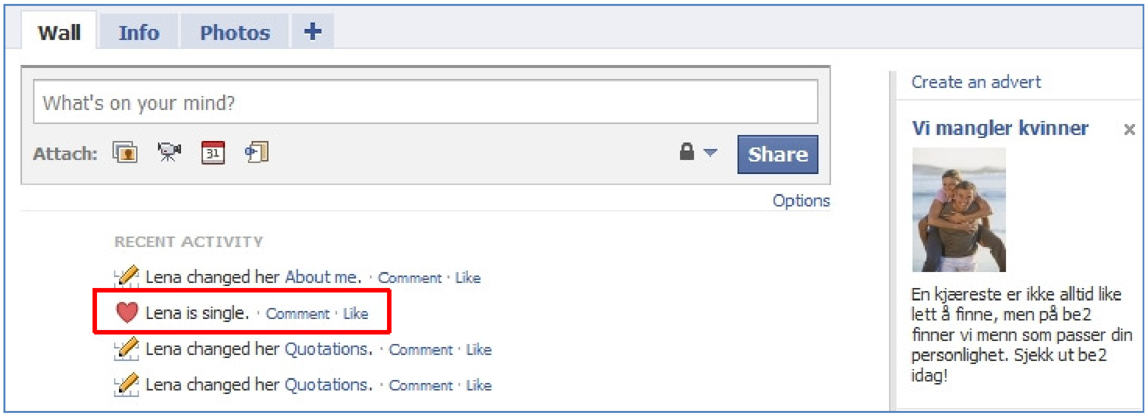
2.3. How are personal data used by Facebook?

With more than 500 million users worldwide, Facebook is now a major participant in the so called *attention economy.* This is, according to Wikipedia, defined as an approach to the management of

[7] Availabe from http://www.schneier.com/essay-322.html

information that treats human attention as a scarce commodity, and applies economic theory to solve various information management problems.[8] The more personal information Facebook members leave on their profile, the more attractive Facebook becomes for advertisers and other third parties who want to reach new potential customers. It is expected that Facebook's revenues will exceed 1 billion dollars in 2010.[9]

When we started adding personal information to our Facebook profile we experienced an immediate change in the nature of the advertisements appearing on our profile. For example, when we provided information to Facebook that we were single, we received ads from dating companies in the sidebar in our profile. And soon after we shared a link about Rome, we received an offer for a weekend in Rome.



Lena changed her About me. · Comment · Like

Lena is single. · Comment · Like

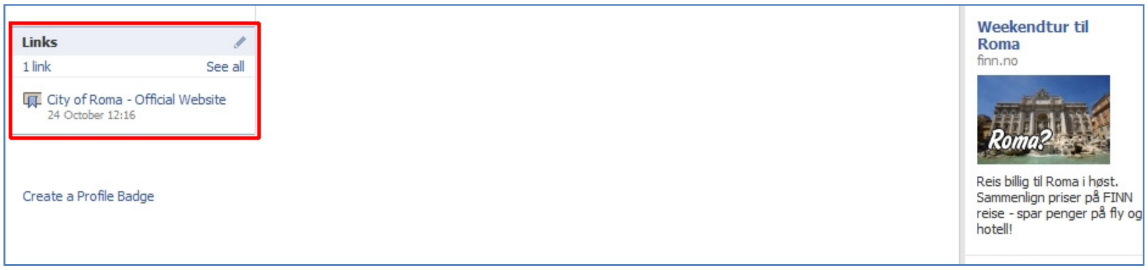
Lena changed her Quotations. · Comment · Like

Lena changed her Quotations. · Comment · Like

Vi mangler kvinner

En kjæreste er ikke alltid like lett å finne, men på be2 finner vi menn som passer din personlighet. Sjekk ut be2 idag!

Figure 6: Lena is now single - the advertisement is for Be2, a dating service



City of Roma - Official Website
24 October 12:16

Weekendtur til Roma
finn.no

Reis billig til Roma i høst. Sammenlign priser på FINN reise - spar penger på fly og hotell!

Figure 7: We shared a link to a site City of Rome – and got an ad back

In our point of view, these examples give a simple indication of the purposes for which the information that the users are providing, are being handled and processed. The exact processing operations, however, remain unknown to us, although reference can be made to section 5 of the Privacy Policy, and to the *Facebook Advertising Guidelines*.

[8] http://en.wikipedia.org/wiki/Attention_economy
[9] http://www.insidefacebook.com/2010/03/02/facebook-made-up-to-700-million-in-2009-on-track-towards-1-1-billion-in-2010/

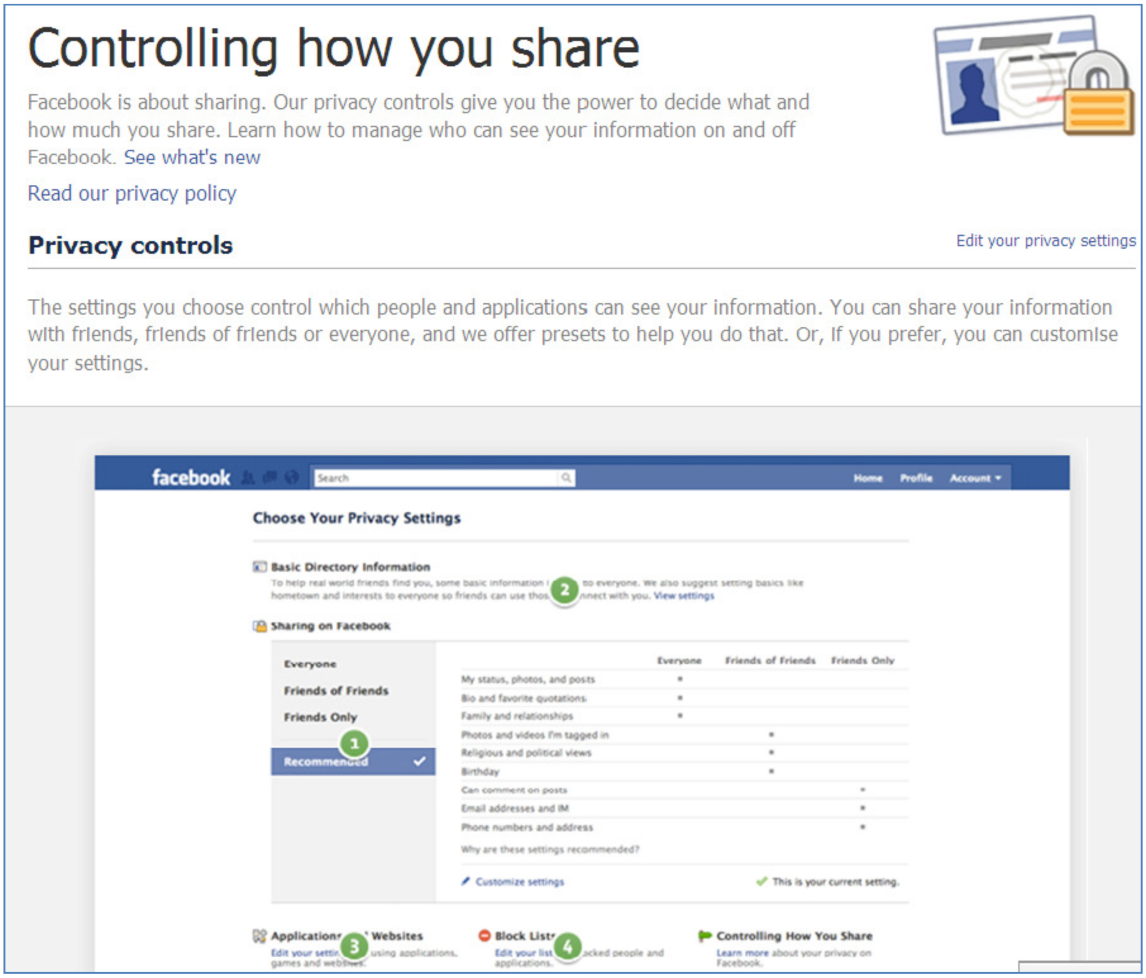
3. Facebook's Privacy Policy

3.1. Description

The Privacy Policy consists of nine paragraphs, each containing the word "*information*", except for the introduction, and the final section labelled "*Other terms*". In these paragraphs, the word *information* refers to information about us – the users, or members of the Facebook community. These paragraphs are distributed across approximately ten pages.[10] To Norwegian users, the policy is in English by default, but French, German, Spanish, Italian and Turkish versions are also available.[11]

Facebook's Privacy Policy can be accessed at any time from the Facebook interface, by clicking the link "*privacy*" on the bottom corner of the screen, at the right hand side. By doing so, you are in fact first taken to a set of guidelines, which are relatively accessible compared to the Privacy Policy itself.

This is how it looks:



Controlling how you share

Facebook is about sharing. Our privacy controls give you the power to decide what and how much you share. Learn how to manage who can see your information on and off Facebook. See what's new

Read our privacy policy

Privacy controls

Edit your privacy settings

The settings you choose control which people and applications can see your information. You can share your information with friends, friends of friends or everyone, and we offer presets to help you do that. Or, if you prefer, you can customise your settings.

facebook

Search

Home Profile Account

Choose Your Privacy Settings

Basic Directory Information

To help real world friends find you, some basic information i to everyone. We also suggest setting basics like hometown and interests to everyone so friends can use thos nnect with you. View settings

Sharing on Facebook

Everyone

Friends of Friends

Friends Only

Recommended ✓

	Everyone	Friends of Friends	Friends Only
My status, photos, and posts	•		
Bio and favorite quotations	•		
Family and relationships	•		
Photos and videos I'm tagged in		•	
Religious and political views		•	
Birthday		•	
Can comment on posts			•
Email addresses and IM			•
Phone numbers and address			•

Why are these settings recommended?

Customize settings

✓ This is your current setting.

Applications Websites

Edit your settin using applications, games and websites.

Block Lists

Edit your list acked people and applications.

Controlling How You Share

Learn more about your privacy on Facebook.

Figure 8: Controlling how you share

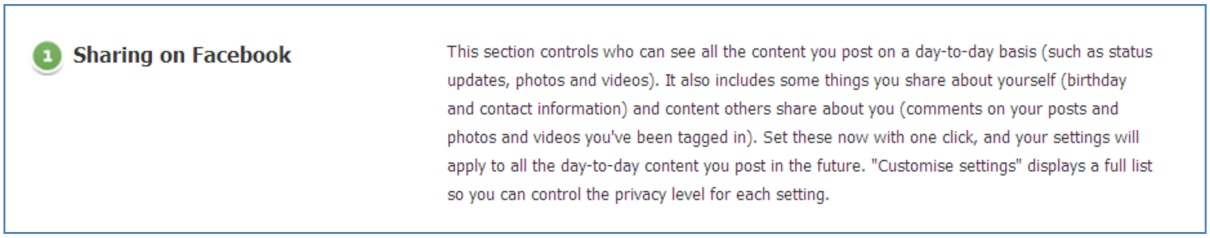
[10] Pages counted after the text was copied and pasted into a word document, using Arial 10 pt. font and a spacing of 0.

[11] As of the 5th of October 2010.

These guidelines consist of four main sections, that each refers to the numbered dots in figure 8 above:

1) "Sharing on Facebook"
2) "Connecting on Facebook"
3) "Applications and websites"
4) "Block lists"

Under each of these points follows a short description corresponding to the section marked by the numbered dot, for instance:



1 Sharing on Facebook

This section controls who can see all the content you post on a day-to-day basis (such as status updates, photos and videos). It also includes some things you share about yourself (birthday and contact information) and content others share about you (comments on your posts and photos and videos you've been tagged in). Set these now with one click, and your settings will apply to all the day-to-day content you post in the future. "Customise settings" displays a full list so you can control the privacy level for each setting.

Figure 9: Explanation of the concept of sharing

As it appears from the screen shot in figure 8, the user is either directed towards the complete *Privacy Policy*; alternatively he or she can proceed to edit his or her own privacy settings, or continue to read the pages on controlling how information is shared.

In the following paragraphs, we shall look into the Privacy Policy, and some of the other statements and documents concerning the users' privacy.

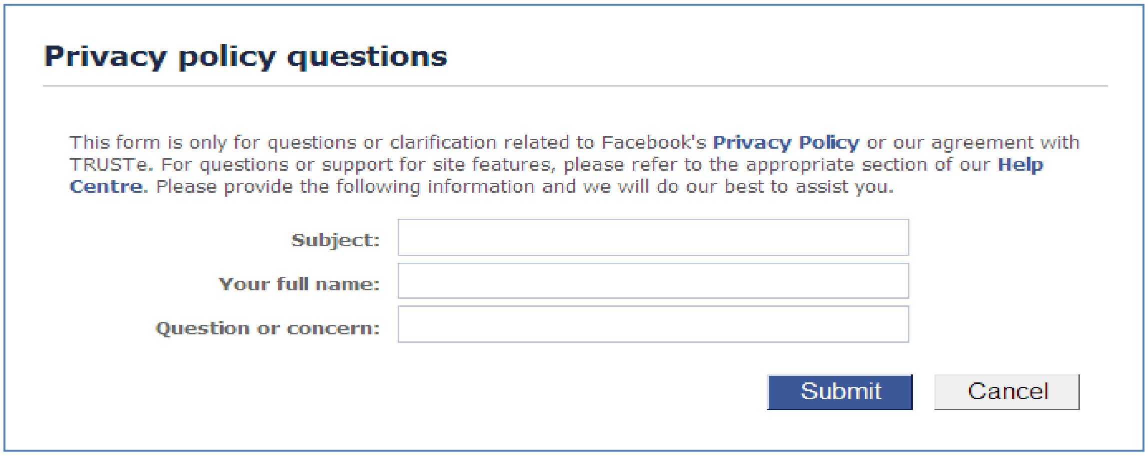
3.2. Relevant documents

The *Privacy Policy* appears to be the main document providing information on the processing and protection of the users' personal data. However, other documents are also relevant in this regard – the policy contains numerous hypertext references to information both inside and outside of Facebook.

We have found, amongst others:

1) TRUSTe web site / TRUSTe Privacy Program Requirements
2) Department of Commerce's Safe Harbour web site
3) Facebook's Statement of Rights and Responsibilities
4) The About Platform page

It is, incidentally, possible to address questions regarding Facebook's privacy practices directly to Facebook by conventional mail, or through a designated help page:



Privacy policy questions

This form is only for questions or clarification related to Facebook's **Privacy Policy** or our agreement with TRUSTe. For questions or support for site features, please refer to the appropriate section of our **Help Centre**. Please provide the following information and we will do our best to assist you.

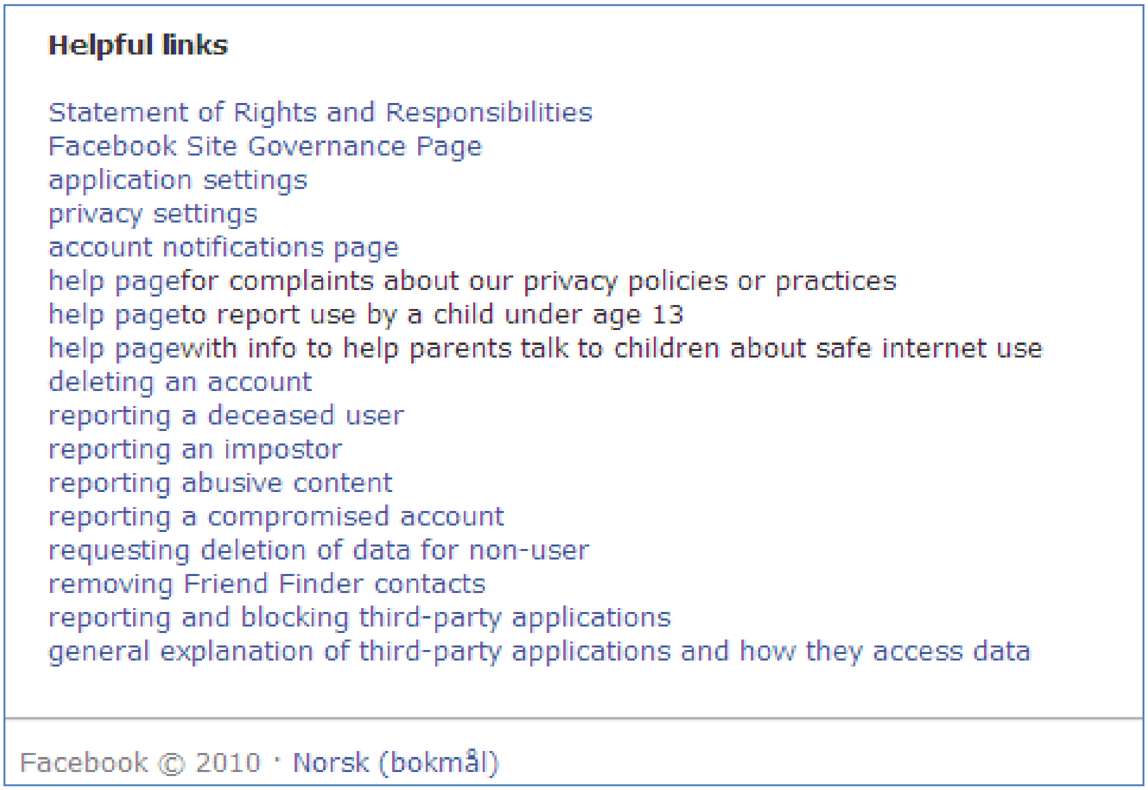
Subject:

Your full name:

Question or concern:

Figure 10: How to contact Facebook for guidance in questions regarding the Privacy Policy

Numerous references are made throughout the policy to different help pages, from which the users can delete their accounts, remove contacts imported via the "*Friend Finder*", and so on. Also, the privacy settings page is referred to quite frequently throughout the policy. At the end of the document, there is a complete list of links to the pages that are in some way or another relevant for user privacy:



Helpful links

Statement of Rights and Responsibilities
Facebook Site Governance Page
application settings
privacy settings
account notifications page
help pagefor complaints about our privacy policies or practices
help pageto report use by a child under age 13
help pagewith info to help parents talk to children about safe internet use
deleting an account
reporting a deceased user
reporting an impostor
reporting abusive content
reporting a compromised account
requesting deletion of data for non-user
removing Friend Finder contacts
reporting and blocking third-party applications
general explanation of third-party applications and how they access data

Facebook © 2010 · Norsk (bokmål)

Figure 11 Links to various pertinent documents

The overall impression is that Facebook presents its users with a relatively detailed set of information. Sometimes the message is clear and, in our assessment, relatively easy to grasp. But the wording can also be vague, and the actual consequences of the statements can be difficult to comprehend. To get the full picture, one is also sometimes required to read the Privacy Policy in light of the Statement of Rights and Responsibilities, and *vice versa*.

Below, we will examine more thoroughly the contents of the policy, and its adhering documents.

3.3. What the documents and statements say

3.3.1. Privacy policy

The policy is divided systematically into different parts, following a certain methodology of categorization. The policy is, inter alia, giving the reader a presentation of the nature of the information that Facebook receives, or otherwise processes. It is also explained how this information is used or distributed in different contexts. Reading the Privacy Policy should, in the end, enable you to manage your own privacy settings. Thus, the users can gain control over the circle of persons who can access their personal data, how this information is protected, and so on.

The policy's table of contents is as follows:

1. Introduction
2. Information We Receive
3. Sharing information on Facebook
4. Information You Share With Third Parties
5. How We Use Your Information
6. How We Share Information
7. How You Can Change or Remove Information
8. How We Protect Information
9. Other Terms

3.3.1.1. Scope of the policy

According to the introduction, the Privacy Policy "*covers all of Facebook*". An important exemption concerns "*entities that Facebook does not own or control, such as applications and websites using Platform*". It is in this section of the policy that the user confirms that he or she agrees to the Facebook privacy practices.

One question that follows in the wake of the quoted phrases is about Platform – what is Platform? This phenomenon is not explained or defined in the policy itself, but it becomes clear later on, in paragraphs 2 and 4 of the policy, that it has got something to do with third party applications and websites.

The Facebook user will, in other words, need to acquire more information about this *Platform* to be able to fully understand the extent of the limitations of the policy's scope.

3.3.1.2. Information about yourself

Under this section, the nature of the information that Facebook collects is presented, and here the readers encounter a clause that can offer some challenges when it comes to its interpretation. Facebook first states that certain personal information is mandatory, and then Facebook proceeds with the following: "*In some cases we may ask for additional information for security reasons or to provide specific services to you".*

The use of the verbal auxiliary "*may"* expresses incertitude, and ideally, this point should be clarified, in our opinion. On the other hand, since Facebook says that it "*may ask*", one is given the impression that you will be presented with a choice as to whether you would like to give your permission or not, when such eventualities – "*some cases*" – arise.

Another aspect is that Facebook lets you inform your friends and the whole Facebook community of your political or religious views. According to Norwegian and European legislation, these are examples of special categories of data, often referred to as *sensitive data*. There are no formal restrictions that prevent us from consenting to the processing of such data, but if somebody encourages the disclosure of such data using automatic or electronic means in the process, this may entail that the processing needs to be approved by the pertinent authority.

3.3.1.3. Friend information

Under this section, the so called "*Friend Finder*" is referred to. As use of the "*Friend Finder*" requires you to provide your password to one or more of your e-mail accounts, Facebook makes it clear that your passwords will not be stored after your friends have been uploaded.

This makes sense to us, but is the user given this information when he is first presented with the "*Friend Finder*" function? The offer of finding your friends through an e-mail account appears shortly after the sign up procedure has been completed, and we believe it would be appropriate to provide this information when the user is presented with this opportunity.

3.3.1.4. Information about site activity, access device and browser

Facebook keeps track of "*some of the actions you take on Facebook*", and it gives examples of such actions. These can be adding connections, creating a photo album or poking another user. Then it is stated that "*[i]n some cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content, we might log the fact that you shared it*".

Facebook also informs us that it "*may*" collect information from the device that you used to log on. It "*may*" also collect your IP address, as well as the pages you visit.

Again we see the use of the words "might" or "may". From a Norwegian point of view, this makes us wonder which factors are deciding when this information is logged or collected – is it up to the employees of Facebook to decide, or are there certain automated procedures? Does this imply that the user can control whether his or her IP address is collected?

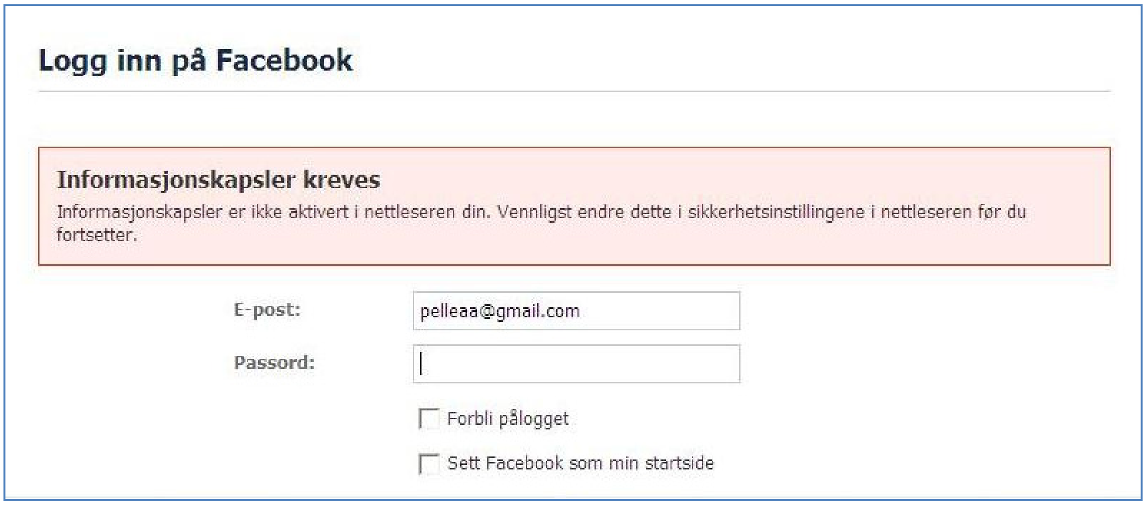
Besides: Does Facebook collect information pertaining to web sites outside of Facebook, that I visit when I am logged on, or when I have logged off? Or does this section only concern Facebook pages?

As far as our experience is concerned, logging on to Facebook with an iPad or iPhone always generates the collection of information about this fact, and furthermore, it is posted on the wall that your posting was made with an iPhone. And our guess would be that IP addresses are *always* collected. As for the "*pages you visit*", the scope of the matter, cf. the question raised above, should be clarified in our opinion.

3.3.1.5. Cookie information

Facebook uses cookies, like the vast majority of websites, and we are informed of this fact. The purpose is "*to make our advertising better, and to protect both you and Facebook*". Maybe there is no way to explain in a simple manner the purposes of the use of cookies. Anyway, the purpose of "protecting" the users and Facebook, strikes us as somewhat vague.

We are informed that cookies can be blocked through our browser settings. We tried to block cookies in our browser settings,[12] and the result was this:



Logg inn på Facebook

Informasjonskapsler kreves

Informasjonskapsler er ikke aktivert i nettleseren din. Vennligst endre dette i sikkerhetsinstillingene i nettleseren før du fortsetter.

E-post: pelleaa@gmail.com

Passord:

□ Forbli pålogget

□ Sett Facebook som min startside

Figure 12: "Cookies required to log in - please activate cookies in your browser"

Apparently, the Privacy Policy is somewhat misleading on this point.

3.3.1.6. Information Facebook receives from third parties

Facebook informs that it receives information from the following:

- Platform – when you engage with a platform application, information about this will be collected
- Other websites
  - "*conversion tracking*" – tracking users' response to ads shown in Facebook
  - Facebook "*may*" receive information about whether you have "*seen*" or "*interacted"* with ads on other websites
- Other users may tag you, or take similar actions, the consequence being that Facebook receives information about you

This raises several questions, in our opinion, for instance the question of explicit and prior consent, a fundamental principle in European data protection law. In this context we refer to the case described later in this document, of the French Data Protection Authority, the CNIL, and Facebook Places.

[12] Internet Explorer.

And, secondly, the collection and storage of information about which websites we have seen, or visited, outside of Facebook can result in a database on vast quantities of data concerning the Internet habits of more than 500 million users.

3.3.1.7. Sharing information

In this section, the users are explained how to adjust the privacy settings, and how our information is distributed when sharing.

According to the policy "*your name and profile picture does not have privacy settings*". This entails that your name and picture will be available to everyone. In this section of the policy, Facebook recommends not uploading, or deleting, your profile picture, if "*you are uncomfortable with this*". On the other hand, as mentioned above, you are encouraged to upload a profile picture during the sign up procedure, and you will be reminded continuously that you can upload a profile picture at a later point.

Besides, users are given options for adjusting the privacy settings, meaning that the amount of information that should be available to search engines, other Facebook members or indeed your friends, can be controlled.

3.3.2. Statement of Rights and Responsibilities

The Statement of Rights and Responsibilities is in fact the contract that you are entering into when signing up for Facebook – this is the conclusion that can be deduced from the following expression:

> "*By using or accessing Facebook, you agree to this Statement.*"

We are perhaps stating the obvious then, when we say that this Statement should be read and examined closely.

3.3.2.1. "Ownership" of the personal information and the meaning of "sharing with other"

Under the second paragraph of the statement, entitled "*Sharing Your Content and Information*", we are notified of the fact that "*[y]ou own all of the content and information you post on Facebook".*

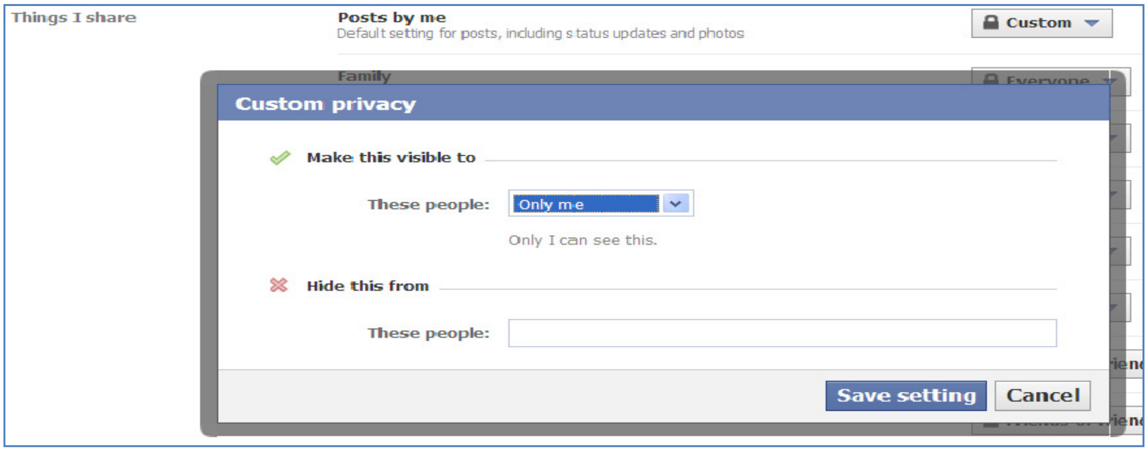
However, this point of departure is significantly reduced in the text that follows. It is pointed out in the Statement clause 2.1 that all users, by using or accessing Facebook, are giving away "*a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License")*. The definition of IP content in this context is content that would otherwise be covered by intellectual property rights.

In principle, we assume that this particular part of the Statement entails that the rights to your profile picture, or any other photo or video of yourself, can either be used by Facebook or handed over from Facebook to any third party with whom Facebook enters into a contract, at any later point in time.

The IP license ends when the IP content is deleted, or if the Facebook account itself is deleted. This is unless the IP content has been "*shared with others*" in the meantime, according to the Statement.

The question that then arises is: In which cases will the IP content *not* have been "*shared with others*", if it has already been posted on Facebook? According to the information we have been given so far, the impression is that posting equals "sharing", and that the "sharing" in question would logically consist of a process that involves more than one person, for example in the form of making some information available to somebody else, who may or may not be your friend; confer the text inside the box in figure 9 above.

Perhaps the sole exception is when the privacy settings are set in the following manner?



Things I share

Posts by me
Default setting for posts, including status updates and photos

Custom

Family

Everyone

Custom privacy

Make this visible to

These people: Only me

Only I can see this.

Hide this from

These people:

Facebook adds that content will be deleted insofar as those you have shared the content with, also have deleted that shared content in particular. This might be regarded as a clarification of the previous wording, in that it could be taken as a presupposition that sharing in this specific context should mean "*first making information available to other people, and then those people downloading that same information*". But what if that "*other people*" are the same people who wish to use that content at a later stage – or what if the IP content is downloaded by Facebook?

3.3.2.2. Deleting information

According to the Statement, deleting information should be understood in as equal to emptying the recycle bin on a computer – that is to say that the information is not really deleted, it is only made unavailable and awaiting to become overwritten.

3.3.2.3. Information being shared with applications

Users are warned that "*content and information*" are shared when using applications. In the receiving end is the application, according to the statement. Our guess is that this would mean that the people or the company who are behind the application, are given access to this information and content.

In any case, which information or content is in fact shared with these applications, is not specified. Considering the fact that the term "*IP content*" has been defined earlier on in the same paragraph – meaning a limited part of this content – it would be natural to assume that the kind of content referred to in this context, is all content no matter what. "Information" presumably includes all personal information available about you or other users.

If one contemplates the potential extent of the distribution that your "*content or information*" might undergo – there are currently 550,000 active applications on the Facebook platform – the whole thing can probably appear to be mildly disturbing.[13]

3.3.2.4. Definitions of terminology

The key terminology of both the Statement and Privacy Policy is defined in this section. This is very useful, both when you are reading the policy and the other relevant documents. Ideally, the user could be presented with these definitions in the Privacy Policy itself, at least in the form of a hypertext reference, since they are highly relevant for the comprehension of this policy.

One concept that is not defined however – and that we would be inclined to classify as crucial, seeing that it has been used on several occasions in the Statement, and that it is decisive in the description of our and Facebook's rights and responsibilities – is "share", or "sharing".

On the other hand, one might be able to deduce what actions are included in the meaning of this term, on the background of the different examples given throughout the *Privacy Policy*. Again, this makes it clear that one needs to consult different documents to get the entire picture.

3.3.3. TRUSTe and Safe Harbour

Under the introductory paragraph of the policy, Facebook ascertains that it "*has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements*."

TRUSTe is, according to Wikipedia

> *"a company based in San Francisco, California, best known for its online privacy seals. TRUSTe operates the world's largest privacy seal program, certifying more than 3,500 websites, including leading online portals and brands like Yahoo, Facebook, Microsoft, Apple Inc., IBM, Oracle Corporation, Intuit and eBay."*

A disclaimer is included at the end of the paragraph:

> *"The TRUSTe program covers only information that is collected <u>through this Web site</u>, and does not cover <u>other information</u>, such as information that <u>may be collected through software downloaded from Facebook</u>".*

Reference is also made to the Safe Harbour framework. This framework is set up between the European Union and the US Federal Trade Commission, to ensure adequate protection of personal data on European citizens, after such data have been transferred from Europe to the US, and it also includes the EEA-countries. From a Norwegian point of view, the general criteria of the Personal Data Act (the Act) also need to be fulfilled before such a transfer can take place – in other words the Safe Harbour scheme cannot be considered in itself as a legal basis for such processing as described in section 2 of the Act, cf. also sections 8 and 9.

[13] If we were to count the amount of web sites that have integrated with Facebook, we would have to add another million. The numbers are gathered from the Statistics page in Facebook's press room (http://www.facebook.com/press/info.php?statistics)

3.4. The Norwegian Personal Data Act

The Personal Data Act is an implementation into Norwegian legislation of the European directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: "the Directive").[14] The Act centres on processing of personal data, and holds the data controller responsible for any unlawful processing of information relating, directly or indirectly, to the data subjects.[15]

A crucial question is whether the Norwegian Act applies to the processing of personal data carried out within the Facebook interface. Another set of questions can be derived from this first question:

- For which processing operations can Facebook be held responsible qua data controller?
- When are personal data processed for private purposes?
- Considering the fact that Facebook is not a Norwegian enterprise – is the Act applicable at all?

The latter question will be dealt with under section 8 of this report. Regarding the first question, The Article 29 Working Party[16] delivered an opinion on online social networking in June 2009,[17] where it discussed whether the provider of the online social networking service (SNS) is to be considered as the data controller in relation to the different processing operations that such SNS providers are offering. Its conclusions were as follows:

> *"[Social Network Service] providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties."*

However, the Party makes a few important exceptions from this point of departure:

- *"Application providers may also be data controllers, if they develop applications which run in addition to the ones from the SNS and users decide to use such an application."*

- *"In most cases, users are considered to be data subjects. The Directive does not impose the duties of a data controller on an individual who processes personal data "in the course of a purely personal or household activity" - the so-called "household exemption". In some instances, the activities of a user of an SNS may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller".*

In its administrative practices, the Data Inspectorate has taken a similar approach.[18]

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[15] The data controller is defined in section 2 no. 4 of the Act as the legal or physical person who determines the purpose of the processing of personal data and which means are to be used.

[16] The Article 29 Working Party is an independent European advisory body on data protection and privacy, set up under Article 29 of directive 95/46/EC.

[17] Opinion 5/2009 on online social networking, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

[18] Cf. the *Gaysir*, *Sukker* and *Biip* cases.

4. Third parties

4.1. Description

According to Facebook, its mission is to give "*people the power to share and make the world more open and connected*".[19] Facebook stresses that it never has and never will sell user information, and expressly prohibits Platform developers from passing any data from Facebook to data brokers.

At Facebook there are not just people and friends, but also companies and third parties that have a commercial angle. In this setting Facebook provides the commercial world with consumer groups.

Facebook puts a lot of efforts into increasing the number of its users, or members. The Facebook application the Friend Finder is heavily promoted with direct connection for catching friends from Windows Live Messenger, Yahoo!, Skype, Wirtualna Polska, hotmail.no, mail.ru and other tools. This service collects the contact list from the member's e-mail program and sends invitations to all contacts.

The advantage for the Facebook member is that it does not need to add all their friends manually when they become a member of Facebook. Facebook will check if the member has friends in the e-mail program's contact list that are not yet a member of Facebook. Facebook will then send an email to the contact where it is also specified who wants you as a friend. In this way, Facebook will expand their customer portfolio even further.

The friend who is in the appropriate contact list is not given the opportunity to opt out of this initiative from Facebook. Facebook will not automatically delete the address after it has been collected; it will be saved for future use.

It is important for Facebook that members add information to their Facebook page. This information can be used for a wide range of commercial services. This information is the basis for dividing members into consumer groups and user groups that will be of interest for third parties.

4.2. Who are the third parties?

The third parties may be divided into different groups. Facebook has offered several services for the third parties and the best way to distinguish them, is by categorizing them according to these different services:

- Ads
- Social plug-ins
- Applications
- Partner sites

We will examine each of these categories more thoroughly in the following.

[19] www.facebook.com/facebook?v=info

4.2.1. Ads

Only application providers and Partner sites have access to member data, beyond what is accessible to everybody.

Advertisers have access to general data, such as:

- Location provided in the user profile (e.g. Oslo)
- Demographics (e.g. age and gender)
- Likes and interests
- Advanced demographics (e.g. birthday, relationship and languages)
- Education and work

Advertisers will be given information on the estimated reach of the advertisement. For instance, there are approximately two and a half million Facebook users living in Norway. Estimated reach will stop at 20 people.

The ad may forward you to a destination, on Facebook or outside, such as a

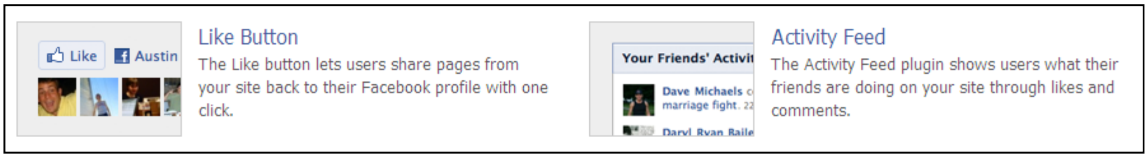
- Page
- Event
- Application
- Group
- Website

Facebook's ad targeting is done entirely anonymously. If advertisers select demographic targeting for their ads, Facebook automatically matches those ads to the appropriate audience. Advertisers only receive anonymous data reports.

4.2.2. Social plug-ins[20]

Social plug-ins are a part of the Facebook Platform. The plug-ins are embeddable social features that can be integrated in a website with a line of HTML. Because they are hosted by Facebook, the plug-ins are personalized for all users who are logged into Facebook.

The most important social plug-in is the *"Like" button*, which enables users to post pages from a site back to their Facebook profile with one click. The "Like" button lets a user share content with friends on Facebook. When the user clicks the Like button on the site, a story appears in the user's friends' News Feed with a link back to the website.



Like Button

The Like button lets users share pages from your site back to their Facebook profile with one click.

Activity Feed

The Activity Feed plugin shows users what their friends are doing on your site through likes and comments.

The Like Box is a social plug-in that enables Facebook Page owners to attract and gain "Likes" from their own website.

[20] The descriptions of the different plugins are quotations from http://developers.facebook.com/

The *Activity feed plug-in* displays the most interesting recent activity taking place on the site. Since the content is hosted by Facebook, the plug-in can display personalized content whether or not the user has logged into the site.

The *Login Button* shows profile pictures of the user's friends who have already signed up for the site in addition to a login button.

The *Recommendations* plug-in shows personalized recommendations to users. Since the content is hosted by Facebook, the plug-in can display personalized recommendations whether or not the user has logged into the site.

The *Live Stream* plug-in lets users visiting a site or application share activity and comments in real time.

The *Facepile plug-in* displays the Facebook profile pictures of users who have liked a page or have signed up for a site.

The *Comments Box* easily enables the users to comment on a site's content — whether it's for a web page, article, photo, or other piece of content.

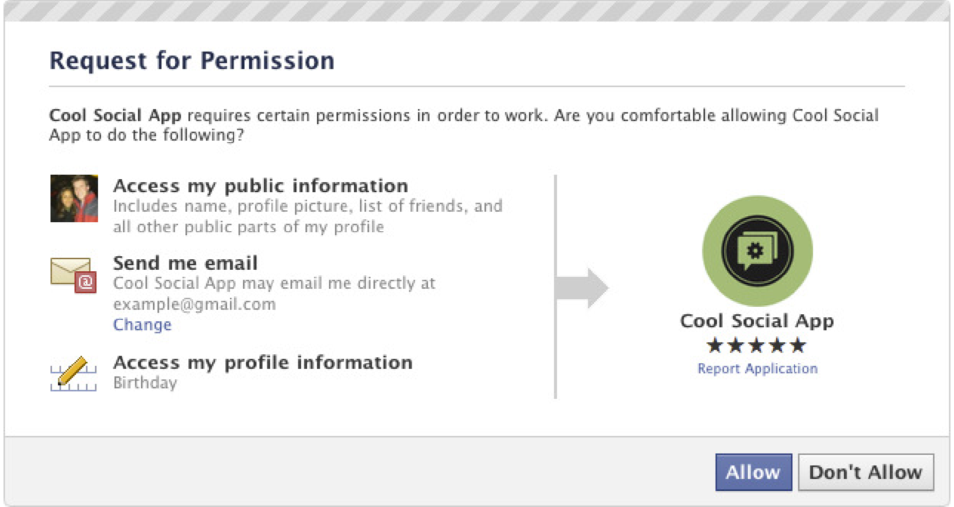
Social plug-ins let the user see what friends have liked, commented on or shared on sites across the web. All social plug-ins are extensions of Facebook and are specifically designed so none of the user's data is shared with the sites on which they appear.

4.2.3. Facebook Connect and single sign-on

Facebook enables users to log in to a third party site with their Facebook account. Once a user logs in to the site with his or her Facebook account, the site owner can access the user's account information from Facebook, and the user is logged in to the site as long as he or she is logged in to Facebook. The site owner gets access to the user's Facebook ID. By default the application can access all public data in a user's profile, including name, profile picture, gender, and friends. If the application needs to access other parts of the user's profile that may be private, or if the application needs to publish content to Facebook on a user's behalf, the application must request extended permissions.

Facebook enables the site owner to remove the registration process for the site by enabling users to log in to the site with their Facebook account. Once a user logs in to the site with his or her Facebook account, the site owner can access the user's account information from Facebook, and the user is logged in to the site as long as he or she is logged in to Facebook.

The open source JavaScript SDK is a simple way to implement login and signup. When a user logs into the site, the SDK saves the credentials for the active Facebook user in a cookie on the site's domain so that the site owner can use the user's identity easily in both the server-side and JavaScript code. It provides a single, simple call-back so the application can automatically handle the complex set of authentication states that exist in a single-sign on system.



Request for Permission

Cool Social App requires certain permissions in order to work. Are you comfortable allowing Cool Social App to do the following?

Access my public information
Includes name, profile picture, list of friends, and all other public parts of my profile

Send me email
Cool Social App may email me directly at example@gmail.com
Change

Access my profile information
Birthday

For example, if a user has previously logged into the website, but doesn't have a cookie for the site in the current browser, the SDK will automatically detect that condition and instantly log the user in to the site without requiring the user to click a Facebook login button again.

The JavaScript SDK requires that the site owner register the application with Facebook to get an app id for the site. The JavaScript API saves the details for the logged in user in a signed cookie. The Facebook login button is only shown for logged out users. The cookie saved by the API also has an access token property in addition to the uid. With that token, the site owner can personalize the site's content to the active user.

Facebook Connect launched in December 2008 and is currently available on more than 15,000 websites, devices and applications, including CNN, CBS.com, Digg, Yelp, YouTube, Xbox, and Nintendo DSI.

The third party receives information about Facebook ID, all public data in a user's profile, including name, profile picture, gender, and friends or request extended permissions.

4.2.4. Account registrations data

Facebook can provide access to all of the basic account registration data that typically will be requested in a sign-up form for a site, including name, email address, profile picture, and birthday. By using Facebook instead of a web form, a new user can provide all of the information required for site registration with a single dialog (no typing required!). Likewise, the information is more reliable than the information from a web form. For example, an email address provided via Facebook has been verified by Facebook, so it does not need to be re-verified by the site.

The third party receives information about name, email address, profile picture, and birthday.

4.2.5. Mobile applications – Facebook SDKs

There are several Software development kits (SDKs) for Facebook. Such as:

- JavaScript SDK

- PHP SDK
- Python SDK
- iOS SDK for iPhone and iPad
- Android SDK

The SDKs enables to access features via different interfaces. One of the most compelling features of SDKs is single sign-on which enables a user to login on to Facebook once, not every time that they use an application.

Mobile Web applications use the same authorization endpoints as normal Web applications, using a special argument (display) to specify the mobile version of the authorization dialog. There are two options for display relevant to mobile Web applications:

- WAP— older mobile Web browsers
- Touch — smart phone, full featured Web browsers

Facebook Platform uses the OAuth 2.0 protocol for authentication and authorization. When a Facebook user authorizes the application, the application gets access to the user's Facebook ID. By default, the application can access all general information in a user's profile, including name, profile picture, gender, and friend list. If the application needs to access other parts of the user's profile that may be private, the application can request extended permissions.

The third party receives information about Facebook ID, all public data in a user's profile, including name, profile picture, gender, and friends or request extended permissions.

4.2.6. Third party applications Facebook

Building an application on Facebook gives a seamless experience as users browse Facebook. The application can integrate with all aspects of the Facebook user experience, from the profile page to bookmarks and the news feed.

Facebook passes information about the user when they interact with the application. Depending on the type of application used, the information can come from different sources.

The application is presented in the Facebook user interface.

Typical is Zynga.com with Farmville.com

The third party receives Facebook ID, all public data in a user's profile, including name, profile picture, gender, and friends, the user's country, the user's locale.

4.2.7. Third party applications – Instant personalization

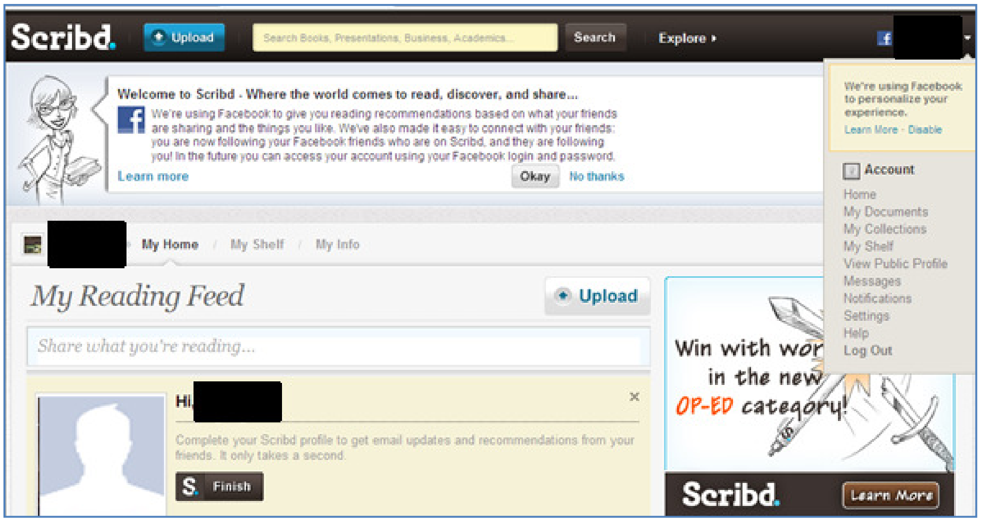
Some select partner sites may access user’s information to personalize the experience as soon as the user arrive, but only information that's already visible to everyone. It is possible to turn off instant personalization for specific sites or to turn it off completely from the Applications and Websites page. This will prevent these partners from receiving information through instant personalization, including what's visible to everyone.

The following websites are partner sites:

- Bing - Social Search
- Rotten Tomatoes - Friends' Movie Reviews
- Docs.com - Document Collaboration
- Pandora - Personalized Music
- Yelp - Friends' Local Reviews
- Scribd - Social Reading

Instant personalization will take information directly from the visitors Facebook profile and use public information to give a personalized experience. In contrast to ordinary third party applications where the user has to sign in, it is possible for the third party applications that use instant personalization to catch and use information from the users Facebook profile without or even before signing up.

Instant Personalization has a big privacy implication since the user does not have to sign in to the site before the site owner knows who the visitor is. The visitor tells straight ahead who he is when entering the site. Because of the big privacy implications the number of Facebook partners is for the time being limited to six.



Welcome to Scribd - Where the world comes to read, discover, and share...

We're using Facebook to give you reading recommendations based on what your friends are sharing and the things you like. We've also made it easy to connect with your friends: you are now following your Facebook friends who are on Scribd, and they are following you! In the future you can access your account using your Facebook login and password.

Learn more Okay No thanks

We're using Facebook to personalize your experience.
Learn More - Disable

Hi, [redacted]

Complete your Scribd profile to get email updates and recommendations from your friends. It only takes a second.

Figure 13 This page was presented when entering www.scribd.com, before even signing in.

The third party receives Facebook ID, all public data in a user's profile, including name, profile picture, gender, and friends or request extended permissions.

4.2.8. Extended permissions

When a Facebook user authorizes an application, the application gets access to the user's Facebook ID. By default, the application can access all public data in a user's profile, including name, profile picture, gender, and friends. If the application needs to access other parts of the user's profile that may be private, or if the application needs to publish content to Facebook on a user's behalf, the application must request extended permissions.

Likewise, to protect the privacy of users who have not explicitly authorized the application, the application will only be able to access the basic profile information about a user's friends, like their names and profile pictures. If the application needs to access other data about a user's friends to enable social functionality, it is necessary to request some of the special friends' permissions listed below.

Applications that request more permission tend to have a lower click-through rate on the permissions dialog. Therefore, you should only ask for the permissions you need from the user at a given time, as you can always ask for more later on.

Extended permissions can be Publishing Permissions, Data Permissions or Page Permissions.

An example on Publishing Permissions is to enable an application to post content, comments, and likes to a user's stream and to the streams of the user's friends. With this permission, it is possible to publish content to a user's feed at any time, without requiring offline access. However, Facebook recommends a user-initiated sharing model.

An example on Data Permission is providing access to the user's family and personal relationships and relationship status.

An example on Page permission is that it enables the application to retrieve access tokens for pages the user administrates. The access tokens can be queried using the "accounts" connection in the Graph API. This permission is only compatible with the Graph API.

The third party receives Publishing, Data and Page Permission, based on consent.

4.3. How does the behaviour-based advertising work on Facebook?

Facebook advertising philosophy is the following:

> *"At Facebook, we believe that every part of our site, including the ads, should contribute to and be consistent with the overall user experience. Thus, we are committed to protecting our user experience by keeping the site clean, consistent, and free from misleading advertising. We believe that we can help transform existing advertising into messages that are tailored to the individual user based on how their friends interact and affiliate with the brands, music artists, and businesses they care about."*

The advertising is tailored to the individual user based on how their friends interact and affiliate with the brands, music artists, and businesses they care about.

Beacon

In November 2007 The Facebook's beacon service included 44 third-party websites. Facebook's starting point was to help members to share information with their friends about what they did on the Internet. Facebook Beacon used a 1x1 pixel GIF web bug on the third party page, and a Facebook cookie. These elements made it possible for Facebook to present to member's friends, what the member had previously done on the internet. This meant that some activity was revealed to friends without the member wanted to tell this.

After strong pressure from members of the Facebook service, the beacon service was first modified and then removed entirely. One thing is that Facebook no longer is able to present to the user's friends that the member had visited certain Web sites, another factor is that Facebook does not then have the opportunity to collect this information for their own benefit. However, there are other services that offer an approximate solution, namely the "like" function.

Facebook does not inform about how the information, on different activities, are weighted. Which ad that is chosen and which that is neglected towards a user is unclear. How an ad is presented for the user is probably complex.

4.4. Cookies

Cookies are pieces of data containing information about web pages that users look at, that are stored in the user's web browser by sites. Facebook uses cookies. The cookie contains uid that is the user ID associated with the cookie.

Facebook knows who you are from your cookie. It's not possible for other site owners to "read" a Facebook's cookie.

Facebook use "cookies" to store the users login ID to make it easier to login to Facebook. Cookies are also used to confirm that the user are logged into Facebook, and to know when the user are interacting with Facebook Platform applications and websites, widgets, Share buttons, and advertisements. Removing or block cookies may impact the ability to use Facebook. Facebook does not share personally identifiable information with advertiser without permission from the user.

4.5. Places

Facebook places is a Facebook application where you may tell your friends where you are. You have to click "Check in" and select the place where you are nearby, from the "nearby places" list. It is also possible to tag friends who are with you at any given location as long as you are checked-in and they have set their privacy settings so they can be tagged. You are asked to write an optional description of what you are doing at the place.

Places are imported automatically to the places application or users create new places by themselves.

All developers have read & write access to authorized users' check-ins, the authorized user's friends' check-ins and information about places. Developers can access, publish, and search the Facebook check-ins of their applications' users. Developers can also search for nearby friends and businesses. A developer's ability to access data is dependent on users and their friends' privacy settings.

Location data is available through the Graph API. For mobile developers, the Graph API requires use of Facebook's new iOS and Android SDKs. User checkins and friends' checkins provides read access to the authorized user's check-ins or a friend's check-ins that the user can see. The Developer Principles and Policies outline Facebook's data storage policies, which also apply to location data. Location data is placed under the extended data permissions, se extended permissions above.

Applications, like maps, request and receive access to the user's location information through a labelled permissions dialog. The only way to avoid sharing location information with an application is to avoid installing it.

5. Default settings

5.1. Information available for other FB-users

Facebook operates with four categories of visibility under the privacy settings. The first category is **Everyone**, meaning that information will be accessible to everyone who is on the Internet (not only on Facebook). The second category is **Friends of friends**, meaning your friends and their friends. The third category is **friends** (self explanatory) and the last category is named **customize**. When choosing this last category you can limit the visibility making the information only available for yourself. Name, profile photo, gender and networks will always be visible for everyone on the Internet and this cannot be changed in the privacy settings.

Additionally the following information is available for everyone on the Internet by default: Status, photos, posts, bio, favourite quotations, family, relationships, sexual preferences, friend list, education and work, current city/town, hometown, likes, connections.

Data	**Default**	**Most privacy friendly option available**
Profile information (name, profile photo, gender, networks)	Everyone	Everyone
Self published information (status, photos etc.)	Everyone	Only me
Family	Everyone	Only me
Relationships	Everyone	Only me
Interested in and looking for	Everyone	Only me
Bio and favourite quotations	Everyone	Only me
Website	Everyone	Only me
Religious and political views	Friends of friends	Only me
Birthday	Friends of friends	Only me
Places I check in to	Friends only	Only me
Tags in photos and videos	Friends of friends	Only me
Contact information (mobile, e-mail etc)	Friends only	Only me

5.2. Information available to third parties

As a Facebook member one can, at least to a certain extent, control the personal information available to third parties. One may also edit other people’s access to your location when using the application “Places”.

The default settings are:

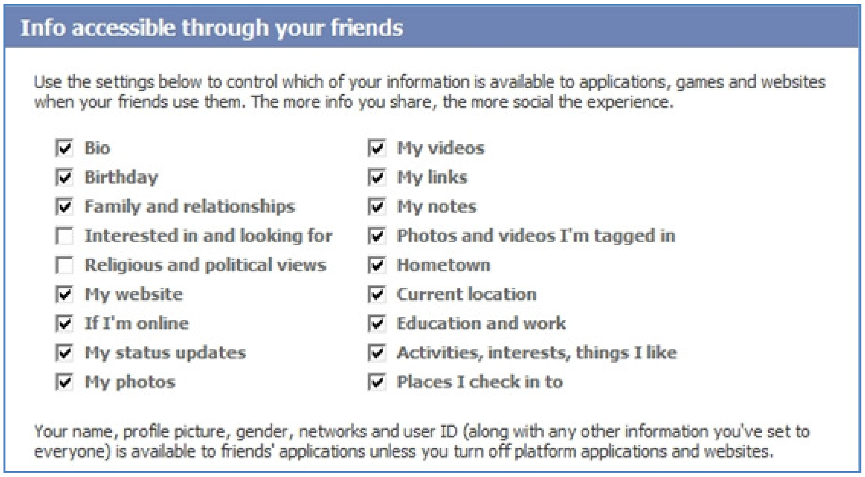
- **Public search engines**
  By default public search engines have access to all of your information open for everyone.
- **Specific partner sites**

By default your account has enabled instant personalisation. This gives Facebook's" specific partner sites"[21] access to all of your information open for everyone.

- **Applications**
  By default applications have access to friends list and any information open for everyone.
- **Places**
  By default people may see your location if they are friends or checked in nearby.

5.3. Information accessible through your friends

By default the following information is available to applications, games and websites when ones friends use them:



Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

☑ Bio
☑ Birthday
☑ Family and relationships
□ Interested in and looking for
□ Religious and political views
☑ My website
☑ If I'm online
☑ My status updates
☑ My photos
☑ My videos
☑ My links
☑ My notes
☑ Photos and videos I'm tagged in
☑ Hometown
☑ Current location
☑ Education and work
☑ Activities, interests, things I like
☑ Places I check in to

Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

Unless one turns off "Platform applications and websites" the following information will always be available for applications, games and websites when friends use them: Name, profile photo, gender, networks, user ID and all other information set to *everyone.*

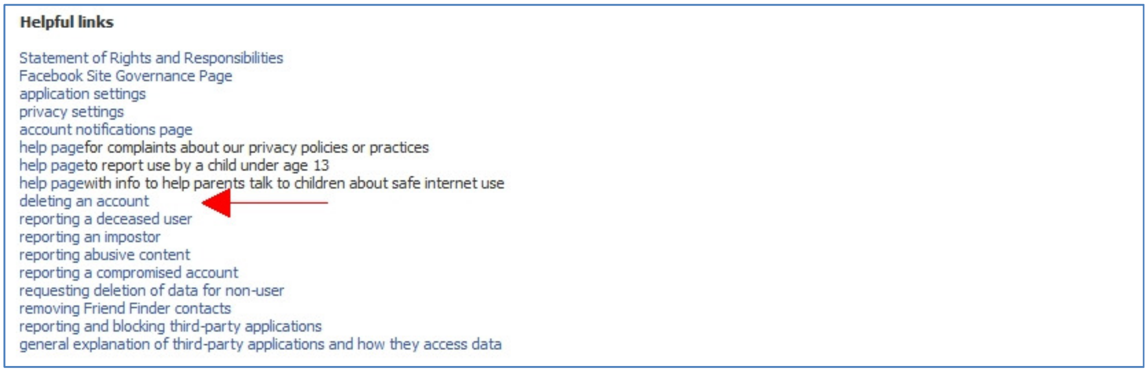
6. Deleting information

6.1. How to permanently delete a Facebook account?

Deleteme.no[22] receives a large amount of inquiries about Facebook, more than any other websites/-services, and the most common question is how people may delete their own profile. Between March 8th and October 31st 2010 deleteme.no was contacted by 209 individuals about this matter. It is not impossible to delete ones profile on Facebook. The challenge is, however, to obtain the information on how to proceed as this information is very well hidden for the common Facebook user.

From ones' own profile site one may deactivate the account, but not delete it. In order to remove it entirely one must follow a link at the bottom of the Privacy Policy document.

[21] http://www.facebook.com/instantpersonalization/
[22] http://www.deleteme.no/english



Helpful links

Statement of Rights and Responsibilities
Facebook Site Governance Page
application settings
privacy settings
account notifications page
help pagefor complaints about our privacy policies or practices
help pageto report use by a child under age 13
help pagewith info to help parents talk to children about safe internet use
deleting an account
reporting a deceased user
reporting an impostor
reporting abusive content
reporting a compromised account
requesting deletion of data for non-user
removing Friend Finder contacts
reporting and blocking third-party applications
general explanation of third-party applications and how they access data

6.2. Is it possible to delete published information?

The short answer to this question is yes. One might delete a comment, photo, message and so on. Thus, it seems more uncertain whether information actually will be deleted when one push the delete button. In October 2010 deleteme.no[23] was contacted by a Norwegian Facebook user who experienced that old information which he had deleted suddenly reappeared on his profile. Does this mean that once you have said you are a Beatles fan you will always be a Beatles fan in Facebook's register? And what happens to deleted information once it has been made available for applications, search engines, advertisers, Facebook's specific partners and so on? These are questions that might be worthy of further studies.

7. International / other authorities

In the following, we present an overview of what steps that we have found that other European data protection authorities have taken vis-à-vis Facebook.

7.1. Denmark

The Danish Data Inspectorate wrote a letter to Facebook in April 2009, in which it addressed several issues. Among these were the deletion of accounts and profiles, hereunder of deceased users, the sharing of information about users with third parties, the retaining of communication and the applicability of the Danish legislation on personal data.

The problem regarding the deletion of Facebook accounts was considered to be of a technical nature, according to Facebook's response.[24]

The Inspectorate also wanted to know whether Facebook considered that the company uses equipment situated in Denmark. At the same time, the Inspectorate referred to the Article 29 Working Party's document on the applicability of European legislation on non EU-based web sites, pointing out that the placing of cookies on a personal computer constitutes the use of such equipment mentioned in article 4 of the Directive.

[23] Deleteme.no is a service from The Norwegian Data Inspectorate. The aim of this service is to help people who experience privacy violations online. The service was launched in March 2010.

[24] In a letter to the Danish Inspectorate dated the 11th of June 2009, Facebook indicated that the problem might be caused by the use of Danish language keyboards.

In response to this, Facebook noted that the Article 29 Working Party's "interpretation of jurisdiction is dangerously overbroad and is inconsistent with the longstanding Safe Harbour agreement between the US and EU".

7.2. Canada

In 2009, The Privacy Commissioner of Canada handled a complaint on the processing of personal data carried out by Facebook.[25] In doing so, it has made an extensive report on its findings. Among the subjects of the complaint were Facebook's default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third-party application developers, and collection and use of non-users' personal information.

The investigation was, according to the Commissioner, focusing on whether "*Facebook was providing a sufficient knowledge basis for meaningful consent by documenting purposes for collecting, using, or disclosing personal information and bringing such purposes to individuals' attention in a reasonably direct and transparent way*."

The Commissioner found that several of Facebook's processing operations were in fact violating the Canadian Personal Information Protection And Electronic Documents Act. The two most noteworthy issues were regarding the default privacy settings and disclosure of personal information to third party applications. Another interesting subject was the Facebook Privacy Policy.

In response to the investigation, Facebook agreed to make several changes. As far as the default settings are concerned, Facebook announced that a "Privacy Wizard" would be introduced in the near future, allowing the users to select between different levels of privacy settings – low, medium or high – in one click. For example, by selecting a high privacy setting, the user is excluded from public search listings.

On the subjects of default privacy settings and advertising, the Commissioner found that Facebook had violated the provisions of the Canadian the Act, but concluded that the problems were resolved on the basis of corrective measures proposed by Facebook.

The Canadian report also concludes that, regarding the subjects of third-party applications, account deactivation and deletion, accounts of deceased users, and non-users' personal information, *"Facebook [is found] to be in contravention of the Act […] In these four cases, there remain unresolved issues where Facebook has not yet agreed to adopt the Commissioner's recommendations. Most notably, regarding third-party applications, the Assistant Commissioner determined that Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers."*

[25] The complainant was the Canadian Internet Policy and Public Interest Clinic (CIPPIC), and the complaint was received by the Commissioner in May 2008.

7.3. Germany

The Data Protection Authority in Hamburg launched legal proceedings against Facebook earlier this year.[26] The matter concerns Facebook's collection of personal data belonging to third persons through the friend finder, i.e. non members of the Facebook community.

The Hamburg authority informed us that Facebook had been very cooperative throughout the process, and that the company had agreed to make several changes to the friend finder function, including the introduction of pop ups with relevant information.

The authority is also of the opinion that Facebook is subject to the obligations laid down in German legislation that is based on the Directive.

7.4. France

In France, La Commission Nationale de l'Information et des Libertés (CNIL) has raised the question whether Facebook Places, one of Facebook's latest services, is in violation of the French legislation in the field of data protection.[27]

Facebook Places allows you to indicate where you are at a given moment, to your friends or indeed to the entire community. The service also allows you to tag your friends in a place, such as a café or a bar. This is done in a manner similar to tagging friends in a picture, thus sharing information about where they are at the moment.

CNIL has pointed out that there are several risks related to our privacy in connection with using the services offered by Places. The main concern seems to be the functionality that allows the users to tag their friends, thus revealing their whereabouts without the person in question necessarily getting immediate knowledge about this. The tagged person will be notified *ex post*, either on Facebook or by e-mail. CNIL regards this notification as insufficient, as the person's consent should always be collected in advance.

In CNIL's opinion, the default settings for Places are unsatisfactory, and there is also a problem related to accessing the privacy settings from mobile units, such as smart phones or iPads. Consequently, CNIL has asked Facebook to improve the default privacy settings, and the information that the company provides regarding Places. In the meantime, CNIL warns the French members of the community to show the utmost vigilance when using Places, and it gives specific recommendations as to which adjustments should be done to the privacy settings.

7.5. Sweden

The Swedish authority, Datainspektionen, has conducted a set of audits of Swedish organizations that were collecting and processing personal data through the use of Facebook.[28] However, the audits did not concern the processing operations for which Facebook is in charge. This initiative resulted in a set of guidelines on the processing of personal data addressed to Swedish governmental, municipal and private organizations and businesses.

[26] http://news.bbc.co.uk/2/hi/8798906.stm

[27] http://www.cnil.fr/la-cnil/actu-cnil/article/article/facebook-places-en-questions-1/

[28] Cf. www.datainspektionen.se/press/nyheter/datainspektionen-granskar-anvandningen-av-sociala-medier/

7.6. The Article 29 working Party

In May 2010, the Article 29 Working Party sent a letter to all signatories of the “Safer Social Networking Principles for the EU”, among which is Facebook. In this letter, the Working Party addresses the problem of third party application providers, and points out that it should be the identities of the service providers on the social networking society should always be transparent. Information about the extent and purposes of any data processing operation should also be presented to the users.

The Working Party underlines

> *“that there is no legal ground for granting a third party application access to the data of user contacts of the user who installs the application, unless the processing can be considered a purely personal or household activity. For the latter case to be applicable there can be no further processing by the third party than the processing explicitly requested by the user who installs the application and all data, including the identifiers of the users’ contacts, needs to be deleted after the processing”.*

And furthermore:

> *“[T]he default privacy settings offered by SNSs should not allow access beyond self- selected contacts and any further access should be an explicit choice by the user. This approach allows for a maximum of control by the user over who has access to his or her profile information and connections list, regardless of the age of a subscribing user […] Apart from restricting access to their profile content, users should have the right to limit the visibility of their presence on the network“*

The Party also stresses that European legislation on data protection is applicable to service providers operating from outside of the EU, provided that it “makes use of equipment” within the context of any processing of personal data.

8. The problem of jurisdiction

The question whether the Norwegian Act applies to Facebook’s processing of personal data, needs to be addressed. If the Norwegian Act is not applicable, the Norwegian Data Inspectorate – which has among its functions to verify that statutes and regulations relevant to the processing of personal data are complied with – would be unable to sanction any violations of the provisions in the Act and its adhering regulations. Section 4 of the Act (which is in line with article 4 of the Directive) states that the Act becomes applicable in two situations.

The first is when the *data controller* is established in Norway. This is clearly not the case with Facebook, as the company lacks any physical presence on Norwegian soil.[29]

[29] According to the Norwegian business register, The Brønnøysund Register Centre, Facebook has no branches or affiliates in Norway, cf. www.brreg.no. Nor is it established in Europe, according to Facebook, in a letter to the Danish Data Inspectorate.

The second is when the controller is not established in Norway, but in a third country[30] – for instance the USA – and the controller makes use of equipment situated on Norwegian territory, for the purposes of processing personal data. This provision is in line with article 4 of Directive 95/46/EC. Whether or not this criterion can be considered to be fulfilled in the case of Facebook, is less obvious.

In the latter case, the Article 29 Working Party has on several occasions announced that it considers the use of cookies to equal the use of such equipment as mentioned in article 4 of the Directive. The corollary being that European legislation on the protection of personal data has a certain extraterritorial effect.[31]

The Working Party pronounces, on the one hand, that it

> *"would advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.*
>
> *With this in mind, the Working Party is of the opinion that not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law. The Working Party has put forward the view that the equipment should be at the disposal of the controller for the processing of personal data."*

On the other hand, the Party believes that

> *"it is not necessary that the controller exercise full control over the equipment. The extent, to which it is at the disposal of the controller, can vary. The necessary degree of disposal is given if the controller, by determining the way how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing. In other words, the controller determines, which data are collected, stored, transferred, altered etc., in which way and for which purpose."*

The Party then proceeds by providing specific examples of when it considers that such equipments are used, in the context of Internet based services. The first example relates to the use of cookies.[32] Through the use of cookies, the service provider is enabled to collect certain information pertaining to the user. For example, cookies are necessary for logon services which offer the possibility of

[30] In this context, the expression *third country* refers to a country outside of the EU/EEA.

[31] Cf. the working document of 30 May 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56). Later opinions communicated by the Working Party refer to this document, see Opinion 5/2009 on online social networking (WP 163) and Opinion 1/2008 on data protection issues related to search engines (WP 148).

[32] Also known as *web cookies, HTTP cookies* or *browser cookies,* cookies are small text files that are distributed from a web server via the visited web site, through the web browser, and ultimately placed on the hard disk of the user's computer. A cookie can contain information on the user's IP address, and information that the user provides when visiting a web site, for instance the user name and password for a logon service. The information contained in the cookie is then sent back to the service provider/data controller.

“remembering” user names. In short, the Working Party concludes that the use of cookies placed on computers situated in Europe, equals the use of such equipment as stipulated in article 4 of the Directive.

The Data Inspectorate has yet to conclude in a case concerning the applicability of the Act in relation to non EU-based web services. We presented the general question about whether the criterion of equipment could be fulfilled through the use of cookies placed on computers in Norway to Dag Wiese Schartum, professor at the Faculty of Law at the University of Oslo. He emphasized that if the SNS exercises control over the software, this software can be viewed as equipment used in the context of the processing of personal data, for which the SNS is responsible *qua* data controller, and it can be deduced that the Act becomes applicable.

From a *de lege ferenda* perspective, he also pointed out that the problem of jurisdiction needs to be resolved temporarily, until the Directive on the protection of individuals with regard to the processing of personal data has been reviewed by EU. Furthermore, as long as the signals from the European Commission are that the use of cookies does trigger applicability of European legislation based on the Directive, the Norwegian authorities should strongly consider to do the same. Such an approach would, of course, also be in line with our common goals that are drawn up in the EEA agreement.[33]

Furthermore, presupposing that European rules were not to become applicable, it would be easy to circumvent European law by way of forum shopping – in other words simply by establishing ones business elsewhere.

However, if European legislation were to become applicable to overseas Internet services, one could encounter a serious problem regarding the enforcement of European – and Norwegian – legislation vis-à-vis these offenders in third countries. If the provisions of the Act are violated repeatedly, and the perpetrators are not willing to accept the sanctions imposed, this could in turn lead to a general lack of respect for the Law, which could be seen as a grave and general problem.

Another possibility, which cannot be derived from the Directive or the national legislation based upon said Directive, is that the problem of jurisdiction is solved by the standards of private international law. Private international law is a set of procedural rules, determining which set of national rules that the resolution of a conflict shall be based upon, provided that the conflict has, in some way or another, a connection to various states. Also determining the location of the competent court is traditionally regarded as part of private international law. The question whether European law applies to Facebook’s processing of personal data on European citizens, consequently, might be dependent upon US standards of resolution of conflicts of law. It should be noted that no initiative has been taken by Norwegian authorities in that direction, neither are we acquainted with any such European initiative.

In all the different alternatives above, we have presupposed that Facebook Inc. in the USA is the controller of our personal data, in the meaning of section 2 no. 4 of the Act, and article 2 (d) of the Directive.

[33] Cf. recital 16 of the agreement.

However, it has lately come to our attention that Facebook Ireland considers itself to be the data controller in relation to the personal data stemming from all European users.[34]

This final alternative brings us back to the criterion of establishment in section/article 4, cf. above.

First of all, the answer would be that the company is not established in Norway, as before. But secondly, and on the other hand, the data processing operations are carried out in the context of the activities of an establishment of the controller on the territory of the Member State, namely Facebook Ireland Ltd.[35]

In this case, the law applicable would be – according to the Directive and the Act – Irish legislation. The following wording from the Statement of Rights and Responsibilities seems to be in support of such an approach:

> *"If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate".*

Consequently, whether Facebook Ireland Ltd. or Facebook Inc. is to be considered the data controller in relation to the data processed concerning Norwegian and European citizens, is a crucial factor. This is not a matter of legal interpretation, but a matter of factual circumstances.

9. Conclusions

9.1. Personal data is a commodity

"It's free, and will always be," Facebook says on its website. Seeing that Facebook is a private company which earns its value from the personal information generated from its users, one might argue that this characterization is not entirely to the point. Facebook makes, after all, money on our personal information, and we "pay" with our personal data and by getting ads in return.

In order to understand the amount of personal data Facebook processes from each of us members, we have in this article divided the processed data into the following ten different categories:

- Mandatory profile data
- Extended profile data
- Personal network data
- Self-published data at home
- Self-published data away
- Other users' data
- Behavioural data
- Connection data
- Metadata and derived data.

[34] The source of this information is

[35] Cf. article 4 (1) litras a and c.

9.2. Facebook is more than a social network site

Besides being a popular site for half a billion people around the world, Facebook has also become present on more and more external web sites through its different social plug-ins, such as the "Like"-button and the "Log-in"-box.

These plug-ins allow the submission of information to Facebook, for example IP-addresses that are collected in the process. This means that Facebook is not only collecting data from its logged-on-users, it is also collecting data from logged-off users and from non-users.

We believe that many web site owners and Facebook users are not familiar with is. The Data Inspectorate will certainly pay close attention to this topic in the near future.

9.3. Legal aspects

By using or accessing Facebook, we agree to Facebook's privacy practices, as they are outlined in the Privacy Policy, and we agree to the Statement of Rights and Responsibilities. Whereas the collection of the mandatory information in the first column of Schneier's taxonomy may be based upon the legal basis found in article 7(b) of the Directive[36], a large part of the data that is being processed is based on the users' **consent** – one of the legal bases on which personal data can be processed, according to the Directive.

However, from a European point of view, the question may be asked if the Facebook consent fulfils the requirements that are given in the Directive, and in the different national laws on data protection.

If we consider the Norwegian Personal Data Act, the definition of a valid consent is given in section 2, which is more or less in line with the definition in article 2 of the Directive:

> *"Any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her."*

It follows from section 8 of the act, which equals article 7 of the directive, that personal data can only be processed on the basis of the individual's consent, provided that the consent is given *prior* to the collection of the information.

On this background, one might ponder whether the Facebook consent would hold up to legal scrutiny from a European perspective. Several questions might be relevant to pose in that regard:

- Is the Facebook consent not, at least partly, a retrospective one?
- Is the user really "informed" after having read the Policy and the Statement?
- What if he or she didn't read the statement at all?
- Can the user give his consent on behalf of another user, as with the *Friend Finder* case?

[36] Its national equivalent being section 8 litra a of the Act.

Perhaps we must accept that we have to give a little of ourselves to take part in the online activities that is social networking – the benefits of this phenomenon should, after all, not be neglected. Nevertheless, after reading the Privacy Policy and the Statement of Rights and Responsibilities, we believe there are two issues that deserve some particular attention.

Firstly: If we had the choice, would we willingly accept that Facebook may collect, and store for an unknown period of time, our IP addresses? When answering this question, one should remember that anonymous or bogus profiles are considered violations of Facebook terms and conditions. In other words, when Facebook collects IP addresses, Facebook is in a position to establish a database of 500 million peoples' IP addresses.

Secondly: The fact that Facebook reserves the right to collect information about the pages we visit, inside and outside of Facebook, deserves some attention. The widespread distribution of social plug-ins all over the web lets Facebook collect information on the pages we see or interact with, without us necessarily even knowing about it. The juxtaposition of our full names, our IP addresses and the web pages we visit, make up a combination of information about Facebook's users, which may be of great interest to a lot of people, for a lot of different purposes.

It is also interesting, in our opinion, to note that there is a certain **lack of transparency,** in general but especially regarding the processing of IP addresses.[37] This leaves us with a great deal of incertitude when it comes to some pretty fundamental queries:

- For how long are our IP addresses stored?
- For which purposes are they used?
- How are these addresses protected – should we have to consider the possibility that this information might be disclosed to third parties?

The same question can be raised regarding the web pages we visit. In relation to both these issues, we certainly believe that the Facebook privacy practices and Statements should be more informative.

[37] The expression ”IP-address” is mentioned only once on the Privacy policy, and not at all mentioned in the Statement of Rights and Responsibilities.