SNS Privacy Requirements

A Framework for Reviewing Privacy Design on SNS

Marin Beijerbacht

WISH WILL WAY
FOUNDATION

Contents

1 Introduction

Social Network Sites (SNS or SN for Social Network) are more popular than ever, with an estimated 4.88 billion users worldwide(1). SNS provide a lot of convenience as people can communicate and share information worldwide. However, due to the world wide adoption and data hungry nature of SNS it has become easy for privacy breaches to occur(2). How privacy is designed into a network is important to minimise the risk users face when using SNS. The privacy design encompasses all parts of the platform that have to do with the processing of data, control thereof and the policies in place(3). How the platform designed these elements into the functionalities and policy offered to users makes the privacy design. Having good privacy design helps users empower themselves to take control over their data and help prevent leakages of user data. Furthermore, when we want to provide meaningful privacy controls and protections the user should be central in the privacy design(4). So not only research on privacy and security is useful, research on the needs and expectations users have regarding their SNS privacy should also be taken into account.

This report aims to do just that. It provides a framework for reviewing and improving the privacy design of SNS. It does this by taking into account both research into the subject of privacy and security and requirements users have regarding privacy design as formalised in (5). The framework can be used to grade different aspects of the privacy design of a SNS platform and in doing so can uncover weak points. Next to quantifying the quality of the privacy design it can help guide the development process of a platform or help improve it. Additionally if repeated more often it can capture the progress of the privacy design and the results can also be shared with the public to increase transparency to users. The following section explains how the framework is structured and how to use it to review the privacy design of a platform. The next section contains the framework and explanations for each requirement. The report closes off with a list of potential further readings for interested readers.

2 User Guide

In this section guidance is given on how to work with the framework provided in this report.

Structure

The framework is divided into 7 categories, each about a different aspect of the privacy design. The categories are Policy and Notice, Information Control, Social Network Practice, Third Party Applications, Security, Information Deletion and Artificial Intelligence. Each category contains requirements for the privacy design. To know what to comply to in order to fulfill each requirement they are subdivided into qualities. These qualities are all small parts that need to be fulfilled in order to comply to the requirement. For each quality it needs to be checked if the platform complies or not. A textual elaboration of each requirement and its associated qualities is provided with the framework.

Where applicable the categories also include some open questions. These are included as some aspects of a platforms privacy design cannot be reduced to a simple yes or no

quality. They are also meant to encourage deeper thought about some aspects of the design on the platform.

Reviewing

A worksheet is available here, which can be filled out and automatically calculates any scores. **To use the worksheet a personal copy should be made before editing.**

The review itself is carried out by going over all qualities provided under a category. For each quality it needs to be decided if the platform under review possesses this quality or not. In the table a *Yes* or a *No* can be supplied depending on the compliance. If any quality is not applicable to the platform under review, because the feature it pertains to has not been implemented, the quality can be marked as *NA*. When using the worksheet *Yes* is a 1 and *No* is a 0, the rest of the grading is elaborated on in the next section.

Next to the filling in of the table, if a thorough review is done, it should be noted down why or how the platform does not comply when it does not have one of the qualities. For any qualities the platform does conform to in a way that is interesting or has changed from a previous version, should note that down as well. This way progress and changes can be tracked over versions if the review is done periodically. The open questions should always be written out of course, unless not applicable.

The review can be done for just the categories of interest or in its entirety, depending on the goal.

Grading

To get an overall grade for a category the score per requirement first needs to be calculated. This score for a requirement can range from 0 to 4 depending on the percentage of qualities that were observed[1]. A 0 is given when none of the possible qualities are observed, 1 for up to 35%, 2 for up to 70%, a 3 for up to 99% and when all qualities are observed a 4 is given.

When a quality is marked *NA*, it can be counted as a *Yes* toward the score of the requirement. This because not having the feature implemented in the first place, it cannot be implemented badly with consequences for user privacy. For example not having a function to upload photos makes it impossible to tag someone in a photo. This would otherwise lead to 'No' for the quality 'Receiving notification when getting tagged'. However with not having the photo functionality in the first place it does not contribute to any privacy weaknesses and actually prevents them.

When the score for all requirements is obtained, the grade for the category (c) can be calculated. This can be done using the simple formula $c = p/t * a + b$. Where p is the sum of points obtained for the category, t is the total of points that could have been obtained for the category, a is the highest obtainable grade and b the lowest obtainable grade. The grade is on a scale from 0 to 10. If all categories have been reviewed the overall privacy grade of the network can be calculated by taking the average of the category grades. The worksheet does all calculations automatically.

[1]The percentage is calculated as follows: (number observed qualities / number total qualities) * 100

3 The Framework

3.1 Policy and Notice

In this category all requirements regarding the user friendliness of privacy and data use policies, as well as notice defaults are contained.

The Requirements and Qualities

- **PN1** - SN users expect simple and user friendly privacy policies.
- **PN2** - Privacy and data use policies should clearly explain how SN user information will be used.
- **PN3** - Users should be informed when any type of linking information or content about them is given or linked by others by default.
- **PN4** - Users should be informed of any type of changes in the Social Network.

Table 1: Qualities needed for each requirement of Policy and Notice

Requirement	Quality
PN1	Clear language is used Reading level suitable to 16 year old Easy to find policy Clear sub sections Concise policy Complementary notice provided Contact information DPO officer included User rights stated clearly
PN2	What data processed clearly explained Purpose processing clearly explained
PN3	Notification tagged in photo by default Notification mention in post by default
PN4	Notification when change in policy Option to opt out in notice

Open Questions

- How is informed consent ensured?

Complying with the General Data Protection (GDPR) already requires that the user should give informed consent(6). In the context of the GDPR this means that the user should be able to know your identity, the purpose of data processing, what data is processed and how. It also entails that the way this information is presented to the user is in plain language, as is captured in the qualities above. However, even though efforts are now being made to make it possible for users to actually understand what is happening to their data, they often do not engage with the information at all. People tend to skip

actually reading the information before consenting(7; 8; 9; 10). This presents the problem of ensuring the user has interacted with the policy in some form, that they are actually informed, before consenting. There is no one right way to ensure your users will actually inform themselves before consenting. Though some things can be done in order to make it easier for them and nudge them to interact with the policies. Please detail what design approach is taken to ensure users inform themselves in some way before consenting.

Elaboration per Requirement

PN1 - SN users expect simple and user friendly privacy policies(11).
To be user friendly, the policy has to be usable and understandable to the user. It is necessary that users understand what they are reading in order for them to give informed consent. For users to be able to understand the policy, the language used should be clear, precise and the sentences should not be overlong(12; 10). There should be minimal use of domain specific or legal terms. Whenever such a term is used, a proper explanation for the term needs to be provided(13). The reading level of the policy should be suitable to a 16 year old. People starting age 16 are allowed to use social network sites and the policy applies to them, so they should be able to read this text and give consent. The readability of a text can be determined using the Automated Reading Index(14). If the platform under review allows younger persons to create an account, for example 13 year olds, the reading level should be such that they can understand it. When presenting the policy to the user, showing all the information contained in the policy at once is very ineffective(15). What is more understandable for users is having not only the full document, but also having a complementary notice containing a summary of the key data practices(16).

Accessibility is the key to usability, without the policy being accessible it cannot provide users with the information it contains. Firstly, to be accessible any link to the privacy policy needs to be easy to find. A font size comparable to that of the rest of the information on the page should be used, preferably underlined and in a contrasting colour to the background. The link should also not be hidden inside other text or otherwise obscured(17). Second, the length and segmentation of the policy count towards accessibility. The longer the policy becomes, the less accessible it is. So short notices when they cover all relevant topics are preferred, thus concise. With segmentation, a clear division and naming of topics covered in the policy creating subsections is intended(17; 18). Next to this, in order to comply with the GDPR and be user friendly, the privacy policy should contain the contact information of the Data Protection Officer (DPO). Also, the policy should clearly state what rights the user has as outlined in the GDPR(6).[2]

PN2- Privacy and data use policies should clearly explain how SN user information will be used(11; 19).
Service providers should inform users about their storage, use and deletion practices. This should happen in a concise and intelligible form, using clear and plain language so it is clearly explained to the user(12). Clear and plain language implies that domain specific

[2]This includes the rights of/to: Information, Access, Rectification, Erasure, Restriction of processing, Data portability, Objection, Avoiding automated decision-making. More information on this can be found here.

terms and legal jargon should be avoided in this explanation(13). To be concise the explanation should be as short as possible. It should express what needs to be said without unnecessary words(20). The users should be informed on what data of theirs is processed and the purpose for this processing.

PN3- Users should be informed when any type of linking information or content about them is given or linked by others by default(21).
When a user B on the platform posts a picture where user A is tagged, user A needs to be notified of this linking information. Same goes for posts by a user B where user A is mentioned. This notifying of user A when user B posts information linked to A should be by default.

PN4- Users should be informed of any type of changes in the Social Network(21).
When the service provider changes a feature of the service that affects how user data is handled, or changes something in their legal documents (terms of service and privacy policy), the user should be notified of this change. The user should be able to decide if they want to continue using the service with the implemented changes. A way to opt out of using the service if the user does not agree to the changes should be provided in the notice(15).

3.2 Information Control

In this category all requirements concerning user control over their data are presented. This contains requirements on data control for not only for visibility of information, it also concerns control over data sharing in relation to third parties and advertisers specifically.

When referring to personal information or personal data, it concerns any information relating to an identified or identifiable natural person. With an identifiable natural person, someone is implied who can be identified by reference to an identifier. Such as name, identification number, location data, online identifier or to one or more factors that are specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person(6). Thus not only name or location are personally identifiable.

The Requirements and Qualities

- **IC1** - SN users should be able to control how their information is collected, deleted, used and shared.
- **IC2** - SN users should be able to determine whether their information is accessible by others, and whether it can be copied or reposted.
- **IC3** - SN users should be able to control the use of their information by advertisers.
- **IC4** - SN users should be able to control the use of location information by location-based applications.
- **IC5** - Users want to see how other users in their network see particular content to find out how much privacy they have.

Table 2: Formalisation of qualities required under Information Control

Requirement	**Quality**
IC1	Controls for what purposes generated data collected and used Controls for what generated data shared with third parties Controls for deletion of generated data Controls for what purposes provided user data used Controls for what provided user data shared with third parties Controls for deletion of provided user data Easy to find controls Clear naming and layout of controls
IC2	Controls for visibility available Granular visibility controls Controls if other users can copy or repost content
IC3	Controls for data use by advertisers Control over what types of data used by advertisers
IC4	Controls for location tracking Still access if location not disclosed
IC5	Option to see profile as outsider

Open Questions

- How are differing (technical) capabilities and backgrounds taken into account?

Not everyone has the same (technical) abilities. Many different types of people, young and old, people with differing disabilities and with differing cultural backgrounds make use of social networking platforms. When it comes to protecting their privacy this can have negative effects if the design of the privacy on the platform does not take an accessible and inclusive approach(22; 23). For example for visually impaired users who rely on a screen reader to navigate the website, if the design of the controls does not support this they cannot take control. Also, the help available to users with their settings is important to help older and less technical users manage their privacy. Please detail what has been done to include the privacy wishes of different populations. What steps have been taken to make the privacy design more accessible and or inclusive?

- Are defaults used for the settings on the platform?

Defaults for privacy settings can have both a positive and negative influence on the welfare of users. Defaults can act as hidden persuaders which can lead to breaches of privacy. When the defaults are applied such that they maximise information sharing, it can make users think that these are in some way better settings or they do not want to make an effort to change them. Which can lead to accidental oversharing. On the other hand, giving active choice to the user and not providing any defaults can be good as it gives autonomy to the user. However, this is not always the best option either, as it requires more effort from the user. It can be that the user does not have any preferences (yet) or is not familiar enough to make such decisions already. Another approach to defaults is a paternalistic one, where defaults are provided such that they protect user privacy for the users own good. Here it can be beneficial, though it can still impede with an users autonomy(24). Please detail what kind of approach to defaults has been implemented on the platform and why this approach was chosen. Do this for the privacy settings and the cookies statement/settings on the platform.

- Are clear pathways provided to users for exercising their user rights?

Under the GDPR users have been afforded certain rights. The platform should supply users with ways to exercise these rights and honour their requests. Please detail for each user right as delineated in the GDPR how the platform facilitates their execution.[3]

Elaboration per Requirement

IC1- SN users should be able to control how their information is collected, deleted, used and shared(25; 26; 27).
The user should be given control over their own information regarding all forms of data processing. Processing is the overarching term for collection, storage, deletion, usage and sharing of data by the service provider(28). Information privacy can be described as "the ability of the individual to personally control information about one's self"(29). To have meaningful privacy decisions for users, the appropriate controls should be provided(15). The controls should enable users to manage the streams of their personal information.

[3]Please find a comprehensive list of user rights and examples of how to implement them here

Giving control and providing functionality can conflict each other sometimes when the data is integral to the functioning of the platform. Control should be given over the data where possible in some capacity.

Two types of data are distinguished for the qualities of this category, namely generated data and provided user data. Generated data is the meta data the user generates by using the platform but does not actively supply themselves, such as sign in times, click rates, inferred advertisement profile. The provided user data is the opposite, this is the data like occupation or phone number that is actively supplied by the user. For the generated data the user should be able to decide for which purposes what data can be collected and used. If some purpose or type of meta data collection is denied then the part of the service that needs it is disabled. For the provided user data the user should be able to control the purposes their provided data is used for. Once again, if some purpose for data use is denied which is necessary for some function on the site, this specific function should be disabled whilst the rest still is available. For both generated and user provided data there should be controls for what can be shared with third parties and controls for the deletion of the data provided. Third parties do include advertisers as well here, even though they are handled separately in IC3 as well.

Any controls that are provided should be usable. They should be easy to reach, which entails that they should not be hidden behind multiple layers of settings. These controls should also have a clear layout and be labelled clearly(30). Clear labelling entails that the name of the setting itself and the level(s) above should be indicative of what can be found there. Following general conventions helps users find the settings they are looking for(31).

IC2- SN users should be able to determine whether their information is accessible by others, and whether it can be copied or reposted(19; 32).
To be able to prevent privacy breaches from occurring users should be able to control, with a high granularity, who sees what of their information(33). With high granularity it is implied that the user can select individual people or groups composed by the user that are allowed access to the information(2). Controls for copying and reposting of posted information of the user by other users should be available as well. This can include blocking or adding watermarks to screen-captured content and blocking the selection of text and download of content.

IC3- SN users should be able to control the use of their information by advertisers(34).
Insight and Controls for the use of personal information by advertisers should be provided to the user. With these controls the user should be able to choose what types of data of theirs may be used for personalisation of advertisements if any.

IC4- SN users should be able to control the use of location information by location-based applications(35).
When using a location-based application or feature on the social network, the user should have control over when the application can receive their location information(36). When not sharing the location it should still be possible for the user to use the parts of the application that do not require the location information instead of being denied access

completely.

IC5- Users want to see how other users in their network see particular content to find out how much privacy they have(21).
To show users how much privacy they have, a feature that shows what their profile looks like to other users, without having to log out, should be included. Users want to know what the effect is of the current visibility settings they have chosen(21). This way accidental oversharing can be minimised(2).

3.3 Social Network Practice

In this category privacy requirements regarding the general business and data collection practices of the provider of the social network are discussed. One requirement on handling behaviour of other SN users is included as well.

Anywhere it is mentioned the user authorise a certain action regarding their personal information, it is implied that this authorisation is given on an informed basis. The user should be clearly informed on what data they are giving the service provider and what processing is done with the collected data.

The Requirements and Qualities

- **SNP1** - SN user information cannot be collected and stored without users' authorisation.
- **SNP2** - Service providers should not analyse, delete or use SN user information for any purpose unless it has been authorised by the user.
- **SNP3** - When SN users provide information for one reason, it should not be used for other reasons.
- **SNP4** - SN user location information should not be disclosed or used for tracking without authorisation.
- **SNP5** - SN users' publicly available information should not be collected or misused by others without their authorisation.

Table 3: Formalisation of qualities required under Social Network Practice

Requirement	Quality
SNP1	User informed on collection and storage practices before authorising No collection of personal information occurs on the service before authorisation (non-users included) No collection of personal information occurs through API/plugin before authorisation
SNP2	Processing of personal data only occurs after authorisation has been given
SNP3	Data used only for the purpose of providing the service Minimal amount of data collected User data not used for financial gain
SNP4	No tracking of user location before authorisation User should be informed of risks when authorising
SNP5	Misuse and collection of data punishable under terms of use Users informed on the risks of posting information publicly

Open Questions

- How can the view of the platform on privacy be described?

Please describe the general view on (informational) privacy of the platform. Creating a concrete description of the stance on (informational) privacy can help contextualise the privacy design on the platform and let users understand if the platform aligns with their standards.

Elaboration per Requirement

SNP1- SN user information cannot be collected and stored without users' authorisation(37; 27).
Before any collection and storage of personal information occurs, the service provider should have received authorisation from the user. This should be done on a basis of informed consent, thus the relevant information should be shown in a digestible manner before the authorisation can be given.
There should not be any collection of data outside of anonymous usage statistics from non-users[4] by the service provider without receiving authorisation first. The collection of personal information by the service provider through other websites, which have an API[5] or plugin of the service in question, should also not occur without prior authorisation of the site visitor.

SNP2 - Service providers should not analyse, delete or use SN user information for any purpose unless it has been authorised by the user(11; 38; 39; 40).
Only once the user has authorised any processing of their data by giving their consent, may any of their personal information be processed. Even then only for the purposes supplied. Under processing fall all actions that can be performed on the data including analysing, sharing and deletion of data.

SNP3- When SN users provide information for one reason, it should not be used for other reasons(41; 42).
The user should be able to trust that the provider will not use their personal information for any purposes outside those given permission for. The reasons for which the personal information is collected by the service provider should be only for the purpose of providing the service. The amount of data they collect should be minimal(6) Using personal information of users for financial gain could be seen as a means for providing the service. However, users do not supply their data to be used as a means of income, they supply the data in order to socialise with people. It is generally in the users interest when personal information is not used for financial gain by the service provider outside of pure provision on functionality(43).

SNP4- SN user location information should not be disclosed or used for tracking without authorisation(35; 41; 27).
Unless specifically authorised by the user in exchange for receiving a certain service, the location of the user should not be tracked or disclosed. The user should be made aware of possible risks when authorising(36). This requirement does not only include GPS as

[4]Persons who are visiting the public features of the service but do not have an account

[5]Application Programming Interface (API), a type of (embedded) application, offering connection to other applications

there are other forms of location tracking as well. Like the IP address, Wi-Fi connection information and Bluetooth information.

SNP5- SN users' publicly available information should not be collected or misused by others without their authorisation(19; 44).
The protection that can be offered for public information is very little, as the user gave this information away publicly themselves. This information is only protected by the terms of service. Misuse of the public information by other users under these terms should be punishable. It however is not always detected, so it remains risky to put personal details in the public domain. What should be done to reduce the risk, is offering granular privacy controls to the user for any piece of information they want to provide[6] and to inform users of risks regarding posting information as publicly available(33).

[6]see IC1 and IC2

3.4 Third Party Applications

In this category all requirements relating to third parties on the platform are presented. Specifically how permissions for data access and informing users of privacy policies for third parties are handled.

The Requirements and Qualities

- **TPA1** - Third parties should not have unauthorised access to SN user information.
- **TPA2** - Service providers should offer a verification function when SN users add a new application developed by a third party.
- **TPA3** - Third party application providers should specify the extent of information collection through their application.

Table 4: Formalisation of qualities required under Third Party Applications

Requirement	Quality
TPA1	Authorisation procedure for third party sharing No access to data before authorisation
TPA2	Third party applications verified by provider
TPA3	Overview of information collected Reason for collection stated and easily accessible

Open Questions

- What third party applications are active/available on the platform?

Please detail which third party services are available on the platform. This is to create a comprehensive list of the places outside of the platform where user data can travel to.

Elaboration per Requirement

TPA1- Third parties should not have unauthorised access to SN user information(45).
Before any communication with a third party server takes place for the first time, the user needs to be informed of the data that will be shared. The user should be able to authorise or deny this data transfer before any exchange takes place(5).

TPA2- Service providers should offer a verification function when SN users add a new application developed by a third party(11).
Before the user can add a third party application, the application should have been verified by the service provider. The service provider should make sure they do not host malicious applications or applications with poor privacy design in order to protect their users(46; 47).

TPA3- Third party application providers should specify the extent of information collection through their application(45; 41; 42).

Before starting the use of a third party application, the user should be provided with a comprehensible overview of the information that is to be collected. The purpose of the collection should also be provided to the user. When the third party does not supply this information to the user themselves, then the service provider should supply this information in an accessible easy to read manner to the user.

3.5 Security

In this category the privacy requirements concerning platform security are discussed. These requirements are about the security measures that are taken to ensure the privacy of user data. Some of these requirements are made to allow for a bit more room regarding the techniques used for security as these change. The elaboration on the techniques used can be discussed in the open questions.

The Requirements and Qualities

- **S1** - SN users should not face identity issues such as false names, impersonation or identity theft.
- **S2** - Information leakage should not occur with mobile or hand-held devices.
- **S3** - SN user information should be well protected so it cannot be leaked through direct attacking techniques.
- **S4** - SN users should be well protected so that they do not receive unwanted communication.

Table 5: Formalisation of qualities required under Security

Requirement	Quality
S1	Security measures taken Educate users on minimizing risk of identity theft Option to report another user Notification when suspicious login
S2	Usable and granular privacy controls on mobile No location sharing or geo-tagging by default
S3	Encrypted data Authentication procedure Ask confirmation when clicking URL Known bad URLs are disabled No data breach in last 6 months
S4	User can specify who can send communications User can remove account from internal search User can remove account from external search User can block other users

Open Questions

- What are the security measures taken on the platform to ensure the safety of users and their data?

Security on SNS is important, on the site scammers can be active and from outside the data they hold on users might be stolen. In order to protect users and their data up to date security is needed. Since the available technology for securing data changes no set

method is given under the requirements, instead here room is provided to elaborate on them. Please detail what security measures are taken and what they guard against.

To get some better ideas of the types of threats to fill in or to see what might still be unprotected see the paper Online Social Networks Security and Privacy: Comprehensive Review and Analysis(48).

Elaboration per Requirement

S1- SN users should not face identity issues such as false names, impersonation or identity theft(41).
To prevent users from having to face identity issues, the service provider should have security measures in place. These security measures can include implementing Captcha services to block automated activity and scanning for other illegal activity like data farming and fake profiles as detailed in the terms of service(49; 50). What specific measures are taken should be detailed in the open questions as these can change depending on the nature of the data and available techniques.

The service provider cannot completely prevent identity issues from occurring when the user is posting inappropriate amounts of personal information publicly. The service provider should educate users on how to properly use the platform with minimal risk and how they can help prevent their information from being exposed unintentionally(46; 50).

In the case that the user was not protected enough and a duplicate account of themselves is active an option to report the account should be available(51). If their account details are stolen and suspicious login activity takes place, the user should be notified.

S2- Information leakage should not occur with mobile or hand-held devices(39).
Leakage of private information can occur accidentally. This can happen if users are not provided the appropriate privacy controls(33). The privacy controls on the mobile version or application of the SN should be granular, usable and accessible[7] in order to prevent accidental leakage of any information. On mobile devices special attention should be given to location information, as more location information is processed and can get leaked(52; 53).[8] Any settings for location sharing or geo-tagging in posts should be turned off by default.

S3- SN user information should be well protected so it cannot be leaked through direct attacking techniques(32).
Basic measures against hacking of information through direct attacks should be implemented to prevent information leakage. The personal information and messages stored should be encrypted(54). To prevent single accounts from being hacked authentication procedures, like two factor authentication (2FA), should be implemented or at least be optionally available to the user(55). The servers any information is stored on should be secured(55; 56). In the open questions the choices for encryption, authentication and further security can be detailed. To help protect users against malicious attacks through URLs, messages asking for confirmation of leaving the platform when the link is clicked should be implemented and links going to known bad servers should be disabled(57; 58)[9].

[7] See IC1 for elaboration on what constitutes clear and accessible controls
[8] The types of location information to be considered can be found in SNP4
[9] eg. through checking it with a blacklist API

As a sign of good security, there should not have been a data leak in the last 6 months. If such a leak occurred, a 0 is to be given given for the entire requirement, as information has not been well protected.

S4- SN users should be well protected so that they do not receive unwanted communication(45; 32; 59).
To prevent unwanted communication, the user should be able to control if everyone or only certain types of users, like friend of a friend, can send friend requests or communications to them. The user should also be able to remove themselves from internal search on the network as well as from external search like search engines, so only people who have their details already can contact them(54). When a user does come across unwanted contact, it should be possible for the user to block the other user(60)

3.6 Information Deletion

In this category the requirements about the practices around the deletion of information on the platform are presented. This includes the retention periods of data and the control users receive for the deletion of their personal information or account.

The Requirements and Qualities

- **ID1** - SN users expect simple and user friendly data deletion processes.
- **ID2** - SN users should be able to delete their information permanently on a per item basis.
- **ID3** - Service providers should not keep SN users' deleted information.
- **ID4** - SN users should know the retention policies for deleted information.

Table 6: Formalisation of qualities required under Information Deletion

Requirement	Quality
ID1	Easy to find information deletion Easy to find account deletion Simple deletion controls
ID2	Deletion procedure for every item Deletion is permanent Account deletion deletes all information
ID3	Upon deletion data is deleted from server Data on backup servers deleted within 30 days
ID4	Retention policy clear and concise How long information kept explained Why information kept explained

Open Questions

- Is there a procedure to get the profile of a deceased person removed?

When someone passes it should be possible for friends or relatives to have the account of the deceased user memorialised or removed. Please detail what procedure is in place on the platform to accomplish this.

Information Deletion

ID1- SN users expect simple and user friendly data deletion processes(52).
Deletion of a piece of personal information or the account should be a simple and straightforward process. The controls for deletion should be easy to find (eg. in a logical well labelled place) and not be hidden behind multiple layers of settings. This goes for both the deletion of individual pieces of posted content and the deletion of the account entirely. It should be clear to the user when they go through the deletion process what information of theirs is selected for deletion, and when the information is officially deleted.

ID2- SN users should be able to delete their information permanently on a per item basis(38; 40).
A deletion process should be available for all provided pieces of information stored on the account. When deleting the complete account, all personal information of the user should be permanently deleted. This is not only for the data the user themselves have provided but also for any generated data about or from the user. Not only should the information stored on the account of the user themselves be deleted, also comments made on the profiles of other users and other linking information should be deleted(61).

ID3- Service providers should not keep SN users' deleted information(19).
Upon deletion of a piece of personal information, this information should not remain on the server of the service provider. For data stored on third party servers, this should also be automatically deleted when requested on the main platform. The backup of this now deleted data should be deleted within 30 days. If this or deletion from third party servers is technically not possible, a reasonable explanation and alternatives should be provided to the user[10].

ID4- SN users should know the retention policies for deleted information(19).
A clear, simple and concise retention policy should be provided to the user(12). Here it should be explained what information is kept on log or backup, for how long it is kept and why the information is kept after deletion.

[10]See ID4

3.7 Artificial Intelligence

This category is in addition to the original requirements as condensed in (5). Here requirements regarding the implementation and use of Artificial Intelligence (AI) on social network platforms are detailed. AI in this report it refers to techniques and algorithms involving some form of machine learning. When an algorithm is mentioned, this can refer to any form of algorithm. Though on SNS algorithms often take the form of curating the content for a user or as a bot, like a chatbot.

The Requirements and Qualities

- **AI1** - Any algorithm implemented should be authorised and transparent about when it operates.
- **AI2** - Users should be able to exert control over the interaction, data collection and data processing done by any algorithm.
- **AI3** - Processing of user data by an algorithm should be secure and minimal.

Table 7: Formalisation of qualities required under Artificial Intelligence

Requirement	Quality
AI1	Informed consent for use explicitly given Information on the data processing of any algorithm used is provided to the user It is transparent what algorithms are used where and when
AI2	Control is given to the user over when any algorithm is active Control is given to the user over what information any algorithm can collect and use Controls for deletion of data profiles and extrapolated data created by an algorithm are provided
AI3	Data collected and used by an algorithm is secured Data collected for the functioning of any algorithm is minimal

Open Questions

- What forms of artificial intelligence algorithms are used on the platform?

Please give a detailed description of all forms of artificial intelligence that are used on the platform. This includes what it does, what data it uses and if any privacy risks are associated with it. Do this for the algorithms from the platform itself and those from third parties used by the platform.

Elaboration per Requirement

AI1 - Any algorithm implemented should be authorised and transparent about when it operates(6; 62; 63).
Before any algorithm starts to process user data, the user should be presented with a clear way to authorise this use(63). This can for example be done by providing notices

that ask for authorisation at each point before an algorithm is used for the first time. In order to make an informed decision about this authorisation of an algorithm, the user should have been clearly presented with what data the algorithm uses(64). This implies that the data use of an algorithm should have been detailed in the privacy notice and in the authorisation notice. Furthermore, it should be transparent to the user when any form of artificial intelligence is used(62; 6).

AI2 - Users should be able to exert control over the activation, data collection and data processing done by any algorithm(6; 65; 62).
To give the user a meaningful form of control over any algorithm, they should be the ones in charge over deciding when it is active or not. Data processing by algorithms can uncover new relations in data and can extrapolate previously unknown data about an individual(66). By deciding if the algorithm can be active users obtain more control over what happens with their own data. Further control should be given to the user about what information of theirs an algorithm may obtain and use. This way the user has control over the data profile the algorithm can access. Next to control over activation and access it is important the user has control over the deletion of the data as well(65). Thus controls for the deletion of any data profiles created for use by algorithms and any extrapolated data by an algorithm should be provided.

AI3- Processing of user data by an algorithm should be secure and minimal(62; 67; 68).
The data used and produced by any algorithm should be stored securely. The data should be stored in an encrypted form. This also should be the case if it is stored on a third party server. In the case of a chatbot, the chat should use end-to-end encryption. Furthermore, wherever possible the data should be anonymised(67). It is good to secure any data stored, however this is not all. It is even better to not collect too much data in the first place. Hence, only the minimal amount of data should be collected and produced(68).

4 Further Reading

In this section a few papers are recommended per section, for those interested in the topic. Whenever possible an open access version of the paper is supplied. If this is not possible it is noted with *via institution*, as it can be accessed through some institutions with a licence.

General

- Gurses, Seda, Ramzi Rizk, and Oliver Gunther. "Privacy design in online social networks: Learning from privacy breaches and community feedback." (2008). Accessible here.
- Kaur, Puneet. "Designing user centric online privacy." Aalto University, Seminar on Network Security. (2011). Accessible here.

Policy and Notice

- Waldman, Ari Ezra. "Privacy, notice, and design." (2018) Accessible here
- Schaub, Florian, Rebecca Balebako, and Lorrie Faith Cranor. "Designing effective privacy notices and controls." (2017) Accessible here (via institution)

Information Control

- Anthonysamy, Pauline, Phil Greenwood, and Awais Rashid. "Social networking privacy: Understanding the disconnect from policy to controls." (2013). Accessible here.

Social Network Practice

- Franzke, Aline Shakti, Iris Muis, and Mirko Tobias Schäfer. "Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands." (2021). Accessible here.
- The worksheet for the framework discussed above. Accessible here.
- Bösch, Christoph, et al. "Tales from the dark side: privacy dark strategies and privacy dark patterns." (2016). Accessible here.

Security

- Hatamian, Majid. "Engineering privacy in smartphone apps: A technical guideline catalog for app developers." (2020). Accessed here.
- Li, Yan, et al. "Privacy leakage analysis in online social networks." (2015). Accessible here.

- Jain, Ankit Kumar, Somya Ranjan Sahoo, and Jyoti Kaubiyal. "Online social networks security and privacy: comprehensive review and analysis." (2021). Accessible here.

Artificial Intelligence

- Fast, Nathanael J., and Arthur S. Jago. "Privacy matters... or does It? Algorithms, rationalization, and the erosion of concern for privacy." (2020). Accessible here
- Tucker, Catherine. "Privacy, algorithms, and artificial intelligence." (2018). Accessible here.

5 Acknowledgements

This work was commissioned and funded by Jake Blok through the Wish Will Way Foundation.
The framework itself is a elaboration on my own bachelor thesis done for the Vrije Universiteit Amsterdam in 2020. It has been revised so it can be used by others and has new up to date sections and research added to it.

References

[1] Statista, "Social media - statistics & facts." https://www.statista.com/topics/1164/social-networks/#topicOverview, 2023.

[2] S. Chen and M.-A. Williams, "Privacy in social networks: A comparative study," *PACIS 2009 Proceedings*, p. 81, 2009.

[3] P. Kaur, "Designing user centric online privacy," in *Aalto University, Seminar on Network Security*, vol. 4, p. 83, 2011.

[4] J. Barrigar, "Social network site privacy: A comparative analysis of six sites," 2009.

[5] M. B. Islam, J. Watson, R. Iannella, and S. Geva, "What i want for my social network privacy," 2014.

[6] E. parliament, "Eu parliament - general data protection regulation (gdpr)." http://data.europa.eu/eli/reg/2016/679/2016-05-04, 2016.

[7] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Communication & Society*, vol. 23, no. 1, pp. 128–147, 2020.

[8] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 203–227, 2005.

[9] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner, "4. americans' attitudes and experiences with privacy policies and laws," *Pew Research Center: Internet, Science & Tech*, 2019.

[10] L. F. McDonald, Aleecia M. Cranor, "The cost of reading privacy policies 2008 privacy year in review," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, p. 543, 2008-2009.

[11] X. Tan, L. Qin, Y. Kim, and J. Hsu, "Impact of privacy concern in social networking web sites," *Internet Research*, 2012.

[12] M. Graber, D. D'Alessandro, and J. Johnson-West, "Reading level of privacy policies on internet health web sites," *The Journal of family practice*, vol. 51, pp. 642–5, 08 2002.

[13] I. Pollach, "What's wrong with online privacy policies?," *Commun. ACM*, vol. 50, no. 9, p. 103–108, 2007.

[14] R. Senter and E. A. Smith, "Automated readability index," tech. rep., Cincinnati university OH, 1967.

[15] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pp. 1–17, 2015.

[16] microsoft, "Privacy guidelines for developing software products and services version 3.1." http://www.microsoft.com/en-us/download/details.aspx?id=16048, 2008.

[17] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '04, (New York, NY, USA), p. 471–478, Association for Computing Machinery, 2004.

[18] E. P. S. Capistrano and J. V. Chen, "Information privacy policies: The effects of policy characteristics and online experience," *Computer Standards & Interfaces*, vol. 42, pp. 24 – 31, 2015.

[19] P. R. Clearinghouse, "Social networking privacy: How to be safe, secure and social." http://www.privacyrights.org/social-networking-privacy, 2011.

[20] "Cambridge university press - meaning of concise in english." https://dictionary.cambridge.org/us/dictionary/english/concise, 2019.

[21] M. B. Islam, J. Watson, R. Iannella, and S. Geva, "A greater understanding of social networks privacy requirements: The user perspective," *Journal of Information Security and Applications*, vol. 33, pp. 30 – 44, 2017.

[22] Y. Wang and C. E. Price, "Accessible privacy," in *Modern Socio-Technical Perspectives on Privacy*, pp. 293–313, Springer International Publishing Cham, 2022.

[23] Y. Wang, "The third wave? inclusive privacy and security," in *Proceedings of the 2017 new security paradigms workshop*, pp. 122–130, 2017.

[24] N. C. Smith, D. G. Goldstein, and E. J. Johnson, "Choice without awareness: Ethical and policy implications of defaults," *Journal of Public Policy & Marketing*, vol. 32, no. 2, pp. 159–172, 2013.

[25] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336–355, 2004.

[26] K. A. Stewart and A. H. Segars, "An empirical examination of the concern for information privacy instrument," *Information systems research*, vol. 13, no. 1, pp. 36–49, 2002.

[27] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: measuring individuals' concerns about organizational practices," *MIS quarterly*, pp. 167–196, 1996.

[28] E. Parliament, "Eu parliament - what constitutes data processing." https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en, 2016.

[29] E. F. Stone, H. G. Gueutal, D. G. Gardner, and S. McClure, "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations.," *Journal of applied psychology*, vol. 68, no. 3, p. 459, 1983.

[30] P. Raschke, A. Küpper, O. Drozd, and S. Kirrane, "Designing a gdpr-compliant and usable privacy dashboard," in *IFIP International Summer School on Privacy and Identity Management*, pp. 221–236, Springer, 2017.

[31] L. Alonso-Virgós, J. P. Espada, J. Thomaschewski, and R. G. Crespo, "Test usability guidelines and follow conventions. useful recommendations from web developers," *Computer Standards & Interfaces*, vol. 70, p. 103423, 2020.

[32] Y. Y. Guo, "The privacy issue on social network sites: Facebook," *Journal of Digital Research & Publishing*, vol. 2, pp. 83–90, 2010.

[33] A. Kuczerawy and F. Coudert, "Privacy settings in social networking sites: Is it fair?," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pp. 231–243, Springer, 2010.

[34] D. P. Commissionar, "Facebook ireland ltd-report of audit (2011)," *Facebook Ireland Ltd Report of Re Audit*, 2012.

[35] J. Y. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, "Location-sharing technologies: Privacy risks and controls," *ISJLP*, vol. 6, p. 119, 2010.

[36] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns.," in *Interact*, vol. 3, pp. 702–712, Citeseer, 2003.

[37] N. Ozer, C. Conley, D. H. O'Connell, T. R. Gubins, and E. Ginsburg, "Location-based services: time for a privacy check-in," *ACLU of Northern California*, 2010.

[38] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009.

[39] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed? privacy patterns and considerations in online and mobile photo sharing," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 357–366, 2007.

[40] R. Wallbridge, "How safe is your facebook profile? privacy issues of online social networks," *ANU Undergraduate Research Journal*, vol. 1, no. 0, pp. 1–8, 2009.

[41] A. Canales and M. Licon, "Issues with social network privacy," 2011.

[42] R. Rizk, S. F. Gürses, and O. Guenther, "Sns and 3rd party applications privacy policies and their construction of privacy concerns.," p. 143, ECIS, 2010.

[43] S. Gurses, R. Rizk, and O. Gunther, "Privacy design in online social networks: Learning from privacy breaches and community feedback," *ICIS 2008 Proceedings*, p. 90, 2008.

[44] M. Pekárek and S. Pötzsch, "A comparison of privacy issues in collaborative workspaces and social networks," *Identity in the Information Society*, vol. 2, no. 1, pp. 81–93, 2009.

[45] T. Taraszow, E. Aristodemou, G. Shitta, Y. Laouris, and A. Arsoy, "Disclosure of personal and contact information by young people in social networking sites: An analysis using facebook profiles as an example," *International Journal of Media & Cultural Politics*, vol. 6, no. 1, pp. 81–101, 2010.

[46] A. Sadeghian, M. Zamani, and B. Shanmugam, "Security threats in online social networks," in *2013 International Conference on Informatics and Creative Multimedia*, pp. 254–258, IEEE, 2013.

[47] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *2012 IEEE Symposium on Security and Privacy*, pp. 413–427, 2012.

[48] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2157–2177, 2021.

[49] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Computing*, vol. 15, no. 4, pp. 56–63, 2011.

[50] W. Luo, J. Liu, J. Liu, and C. Fan, "An analysis of security in social networks," in *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. 648–651, IEEE, 2009.

[51] R. Barati, "Security threats and dealing with social networks," *SN Computer Science*, vol. 4, no. 1, p. 9, 2022.

[52] B. Krishnamurthy and C. E. Wills, "Privacy leakage in mobile online social networks," in *Proceedings of the 3rd Wonference on Online social networks*, pp. 4–4, USENIX Association, 2010.

[53] L. Jedrzejczyk, B. A. Price, A. K. Bandara, B. Nuseibeh, W. Hall, and M. Keynes, "I know what you did last summer: risks of location data leakage in mobile and social computing," *Department of Computing Faculty of Mathematics, Computing and Technology The Open University*, pp. 1744–1986, 2009.

[54] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *IEEE network*, vol. 24, no. 4, pp. 13–18, 2010.

[55] E. Wang, "Social network security: A brief overview of risks and solution," 2009.

[56] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," *Information sciences*, vol. 421, pp. 43–69, 2017.

[57] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, "Malicious accounts: Dark of the social networks," *Journal of Network and Computer Applications*, vol. 79, pp. 41–67, 2017.

[58] C. Hu, T. Yan, J. Chen, and T. Wang, "Trends in web threats: Attackers were more active during holiday season." https://unit42.paloaltonetworks.com/web-threats-malicious-host-urls/, 2022.

[59] S. Bhatnagar, T. Herath, R. Sharman, H. R. Rao, and S. J. Upadhyaya, "Web 2.0: Issues for the design of social net," in *Web 2.0*, pp. 1–14, Springer, 2009.

[60] P. J. Wisniewski, B. P. Knijnenburg, and H. R. Lipford, "Making privacy personal: Profiling social network users to inform privacy education and nudging," *International Journal of Human-Computer Studies*, vol. 98, pp. 95–108, 2017.

[61] P. I. Powale and G. D. Bhutkar, "Overview of privacy in social networking sites (sns)," *International Journal of Computer Applications*, vol. 74, no. 19, 2013.

[62] H. J. Watson and C. Nations, "Addressing the growing need for algorithmic transparency," *Communications of the Association for Information Systems*, vol. 45, no. 1, p. 26, 2019.

[63] A. Giannopoulou, "Algorithmic systems: the consent is in the detail?," *Internet Policy Review*, vol. 9, no. 1, 2020.

[64] G. Burkhardt, F. Boy, D. Doneddu, and N. Hajli, "Privacy behaviour: A model for online informed consent," *Journal of business ethics*, vol. 186, no. 1, pp. 237–255, 2023.

[65] R. Belen Saglam, J. R. Nurse, and D. Hodges, "Privacy concerns in chatbot interactions: when to trust and when to worry," in *International Conference on Human-Computer Interaction*, pp. 391–399, Springer, 2021.

[66] C. Tucker, "Privacy, algorithms, and artificial intelligence," in *The economics of artificial intelligence: An agenda*, pp. 423–437, University of Chicago Press, 2018.

[67] M. Hasal, J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snášel, and L. Ogiela, "Chatbots: Security, privacy, data protection, and social aspects," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 19, p. e6426, 2021.

[68] B. Fazzinga, A. Galassi, and P. Torroni, "A privacy-preserving dialogue system based on argumentation," *Intelligent Systems with Applications*, vol. 16, p. 200113, 2022.