Agentschap voor Innovatie door Wetenschap en Technologie
IWT
SBO Security and Privacy for Online Social Networks

**Document type** | Report
---|---
**Title** | Privacy-friendly ‘model’ privacy policies
**Deliverable Number** | D9.3.4
**Editor(s)** | B. Van Alsenoy
**Dissemination level** | External
**Preparation date** | June 2013
**Version** | 1.0

**Legal Notice**
All information included in this document is subject to change without notice. The Members of the IWT SBO SPION project make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IWT SBO SPION project shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.
The IWT SBO SPION Project

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Participant name</th>
<th>Country</th>
<th>Department</th>
<th>Participant role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KU Leuven</td>
<td>BE</td>
<td>COSIC/ESAT</td>
<td>Coordinator</td>
</tr>
<tr>
<td>2</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DISTRINET</td>
<td>Partner</td>
</tr>
<tr>
<td>3</td>
<td>KU Leuven</td>
<td>BE</td>
<td>DTAI</td>
<td>Partner</td>
</tr>
<tr>
<td>4</td>
<td>KU Leuven</td>
<td>BE</td>
<td>ICRI</td>
<td>Partner</td>
</tr>
<tr>
<td>5</td>
<td>Vrije Universiteit Brussel</td>
<td>BE</td>
<td>SMIT</td>
<td>Partner</td>
</tr>
<tr>
<td>6</td>
<td>University of Ghent</td>
<td>BE</td>
<td>OWK</td>
<td>Partner</td>
</tr>
<tr>
<td>7</td>
<td>Carnegie Melon University</td>
<td>USA</td>
<td>Heinz</td>
<td>Partner</td>
</tr>
</tbody>
</table>

Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 B. Van Alsenoy</td>
<td>KU Leuven, iMinds-ICRI</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contents

1. Introduction ...........................................................................................................................................4
2. Minimum information to be provided: a checklist.............................................................................5
3. Method of presentation..........................................................................................................................8
  3.1 Layering notice..................................................................................................................................8
  3.2 Visual aids .........................................................................................................................................9
4. Do’s and don’ts.....................................................................................................................................11
5. Conclusion............................................................................................................................................13
1. Introduction

One of the aims of the SPION project is to promote the design of privacy-friendly ‘model’ privacy policies for Online Social Networks (OSNs). Building on the legal, social and technical research performed thus far, we have distilled a number of recommendations for the development of such policies. The objective of these recommendations is to promote privacy policies which are not only complete from a legal perspective, but also designed so that users can easily ascertain the level of privacy offered by the OSN.

As already mentioned in a previous deliverable, we have chosen to use the term ‘privacy notice’ instead of ‘privacy policy’ in order to avoid terminological confusion. To be clear, privacy notices are public-facing documents designed to inform individuals of an organization’s data processing practices, as well as any other information required by data protection or privacy legislation.¹

This report starts by providing a checklist of the minimum information which providers of OSN services must provide to their users. Next, it discusses current best practices regarding the presentation of privacy notices. This discussion is then followed by a number of specific guidelines which the drafters of privacy notices should take into account when developing these notices. Finally, a number of conclusions and recommendations will be provided.

¹ The term ‘privacy policy’ is also frequently used in reference to documents which are internal to an organization and which documents the objectives, rules and/or controls it has adopted in order to satisfy data protection and privacy requirements. See B. Van Alsenoy, E. Kosta and J. Dumortier, ‘Legal requirements for privacy-friendly ‘model’ privacy policies’, Deliverable D6.1 of the SPION Project, June 2012, p. 4-5, available at http://www.cosic.esat.kuleuven.be/publications/article-2237.pdf.
2. Minimum information to be provided: a checklist

Articles 10 and 11 of Directive 95/46/EC² specify which information a data subject should receive with regards to the processing of his or her personal data. A distinction is made between two different scenarios: one in which the information is obtained directly from the data subject (art. 10), and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11).

In the context of OSNs, a significant amount of personal data is collected directly from users. Such data include users’ basic profile information (name, age, place of residence, interests, ...), as well as any information which users voluntarily post (on either their own or another user’s OSN page). However, many OSNs also collect a range of personal data indirectly. For example, OSNs typically maintain ‘behavioral data’ about their users, which reflect the user’s activities on the OSN (e.g., frequency of log-ins, location and/or device from which the service is accessed).³ Certain OSNs also collect information which extends beyond the OSN domain, e.g. by collecting information from the user's browser or from cookies stored on the user’s device. Another example of data not provided directly by users is ‘inferred data’, i.e. data which is derived from other data (e.g., by applying profiling techniques).⁴

It is the responsibility of the OSN provider to present users with clear information about all of these data collection and use practices. At a minimum, this information should encompass the following elements⁵:

---
³ One could argue some of the examples provided here concern information ‘collected directly from users’. We would argue however, that any information which is not explicitly solicited from and actively provided by the individual concerned constitutes an indirect collection practice.
1. The **types of personal data** being collected, as well as how they are collected;
   - **Examples:** your profile information, data related to your use of the OSN, information about you shared by other users, endorsements you make (e.g., ‘like’, ‘+1’), ...

2. The **purposes** for which these data are processed;
   - **Examples:** to provide the OSN service, site performance and security, service improvement, direct marketing, ...

3. The **privacy choices** which individuals have - or don’t have - and how to exercise them (e.g., through configuration of privacy settings or ticking of boxes)
   - If users’ data will be used for **direct marketing** purposes, the privacy notice should clearly indicate whether or not users have an ability to opt-out of such marketing. If this is not the case (i.e., acceptance is a precondition for receiving the service), users should be made aware of this and their explicit consent should be obtained.
   - If the provisioning of certain information is **mandatory** whereas other information is **optional**, this should be clearly indicated. Where relevant, individuals should also be informed of the possible consequences of not providing a certain item of information
     - **Example:** the decision to provide a phone number may not be mandatory but can help users to regain access to their account in case they forget their password.
   - Where **default settings** are in place, individuals should be made aware of this and provided with clear information on the implications of current default settings and how to change these settings.

4. Whether the personal data collected by the OSN provider will be disclosed to any **third party recipients** and, if so, the names of these recipients (or at least a clear indication of the categories of recipients involved), as well as the types of personal data concerned and the purposes for which those third parties may process them;

______________________________

5. Information about the user's **rights as a data subject**, which include the right of access, correction, blocking or deletion, together with an indication of how these rights can be exercised;

6. **Contact information:**
   - the official name of the organization behind the OSN and its physical address, as well as any other contact information;
   - contact information for the independent supervisory body to which individuals may complain if they are concerned that their rights have been breached.

7. An indication of how to obtain **more details** regarding the OSN's information handling and processing practices.
   - Additional information might for example include: details regarding security measures adopted by the organization, countries to which personal data is transferred, further details regarding exercise of data subject rights, ...

Offering a comprehensive account of each of these elements requires considerable effort. A lot of information is required, and the desire to be complete can easily result in a lengthy and complex document. Such a document may in turn be difficult for users to understand, thus undermining the core objective of the privacy notice: to achieve an effective communication of privacy practices. The next section will describe several ways in which OSN providers can improve the presentation of their privacy notices in order to reduce risks of ‘information overload’ and facilitate reader comprehension.

---


3. Method of presentation

3.1 Layering notice

In 2003, the International Conference of Data Protection and Privacy Commissioners adopted a Resolution on improving the communication of data protection and privacy information practices.8 This Resolution advocated for the use of ‘condensed format’ privacy notices as a means to improve the communication of privacy-related information. Specifically, the Commissioners considered that communication would be improved by:

- using a short format for providing information, with a limited number of elements (e.g., 6 to 7);
- providing only the basic information up front, while providing clear and easy access to further information;
- using simpler, everyday terminology; and
- standardizing the manner in which notices are provided.9

In 2004, the idea of using ‘multi-layered’ privacy notices received further endorsement from the Article 29 Working Party.10 According to the Working Party, data controllers may spread out the requisite information over different layers, provided that the sum of all the layers offers all the information required by national data protection laws.11 The Working Party proposed the following three-layer structure:

- Layer 1 – the short notice, which comprises

---

o at least the identity of the controller and the purposes of processing;
o any additional information which - in view of the particular circumstances - must be provided up front to ensure fairness; and
o a clear indication as to how to access additional information.

**Layer 2 – the condensed notice, which comprises**
o all the information mentioned under the checklist above, in summary form

**Layer 3 – the full notice, which comprises**
o all the information mentioned under the checklist above in full (i.e., with specificities) as well as any other information required by national laws.¹²

### 3.2 Visual aids

Parsing notice into different layers can help mitigate risks of ‘information overload’. However, organizations can use additional mechanisms to present their privacy notices in a user-friendly way. Appropriate visualization techniques can help improve the effective communication of privacy notices. For example, in its Opinion on Harmonized Notice Provisions, the Article 29 Working Party recommended presenting condensed notices in a table format to improve reader understanding.¹³ A similar approach has been adopted by the US federal government, where federal regulators have released an online ‘form builder’ to generate model consumer privacy notices automatically.¹⁴

Some research suggests that the use of privacy ‘icons’ or ‘nutrition labels’ can enhance user comprehension. Privacy icons (or ‘pictograms’) are simplified pictures representing privacy related-statements, such as whether or not personal data is shared with third parties or

---


used for marketing purposes. A privacy ‘nutrition label’, on the other hand, offers a matrix of information types and usage, drawing inspiration from nutrition, warning and energy labeling.

A recent proposal for the visualization of a multi-layered notice has been made by Van Den Berg and Van Der Hof. In their design information is presented as spokes of a wheel, whereby each spoke represents a basic data protection principle (e.g., collection limitation, data quality, …). By clicking on an individual spoke, users gain access to the second and third layers of information, where they receive more and more in-depth information about each specific aspect of the processing.

18Id.
4. Do’s and don’ts

The previous section illustrated that there are several ways in which the user-friendliness of privacy notices can be enhanced by considering alternative forms of visualization. In this section, we will provide a few basic guidelines for the developers of privacy notices. Regardless of the chosen method(s) of presentation, adhering to the following guidelines will help improve the effective communication of the contents of privacy notices.\(^\text{19}\)

a. Mind your language

**Do:**
- adopt a simple, conversational style;
- use vocabulary that is readily understood by your intended audience\(^\text{20}\);
- be specific and illustrate by using concrete examples (condensed/full notice).

**Don’t:**
- use technical or legalistic language;
- use vague or open-ended language.

b. Be objective

**Do:**
- use neutral and objective language;
- offer a factual and accurate account of the organization’s practices.

**Don’t:**


\(^{20}\) The US Department of Health and Human Services has developed a ‘thesaurus of Plain Language Words’ and Phrases for HIPAA Notices of Privacy Practices, which illustrates how technical terms can be substituted by common vocabulary (see note 19).
- use suggestive language to instill a sense of confidence;
- give people the impression that they have a choice when they don’t;
- frame privacy choices in a confusing or deceptive way.

**c. Design with care**

**Do:**
- apply a clear structure;
- clearly identify main points;
- parse information into logical groups;
- use a format/size which is appropriate to the medium.

**Don’t:**
- provide too much information at once;
- engage in unnecessary repetition.

**d. Display in a prominent and timely fashion**

**Do:**
- display privacy notices in a clear and conspicuous manner at all times;
- actively communicate the notice when users are asked to provide information and/or exercise their privacy preferences;
- in case of a ‘short’ or ‘condensed’ notice, ensure easy access to more comprehensive statements.

**Don’t:**
- assume that mere availability of the notice is sufficient;
- hide privacy notices (e.g., by using fine print, only making it available after navigating several pages)

**e. Test usability**

**Do:**
- conduct testing to ensure that readers find your notice comprehensible and user friendly;
- reiterate notice in light of user feedback.

**Don’t:**
- limit the review of your notice to technical or legal privacy experts.
5. Conclusion

There are many pitfalls undermining the effective communication of information contained in privacy notices. Some of these pitfalls can be avoided more easily than others. For example, organizations can easily limit the use of technical jargon or ‘legalese’, just by making a conscious effort. Another way in which organizations can enhance the usability of privacy notices is by presenting information in a more user-friendly way.

Several initiatives have been taken to improve the presentation of privacy notices. Many of them recommend ‘layering’ privacy notice as a way to combine meaningful transparency with user-friendliness. Other efforts focus on the use of alternative visualization techniques (such as icons) as ways to improve the communication of information contained in privacy notices.

When designing a privacy notice, one should remain mindful that transparency has a value independent of individual choice. While efforts must be made to present information in a user-friendly way, the notice must remain sufficiently detailed to enable real scrutiny and accountability of OSN providers.

---

21 For a general discussion see B. Van Alsenoy, E. Kosta and J. Dumortier, ‘Legal requirements for privacy-friendly ‘model’ privacy policies’, l.c., p. 16 et seq.