Patterns to support the development of privacy policies

Luanna Lopes Lobato  
Dept. of Computer Science  
Federal University of São Carlos  
São Carlos – SP– Brazil  
luannalopeslobato@gmail.com

Eduardo B. Fernandez  
Dept. of Computer Science and Eng  
Florida Atlantic University  
Boca Raton, FL, USA  
ed@cse.fau.edu

Sérgio Donizetti Zorzo  
Dept. of Computer Science  
Federal University of São Carlos  
São Carlos – SP– Brazil  
luannalopeslobato@gmail.com

Abstract—This paper presents patterns for privacy policies to be used in web sites, in particular e-commerce and e-business sites. Because of their financial aspects, the users accessing those sites need to provide personal information, and expect integrity, security, and privacy. The patterns are derived from a study of the 33 most accessed e-commerce sites in Brazil, where it was possible to observe that they do not use a systematic approach to develop privacy policies which are clear, friendly, and with relevant contents.

Patterns, policy, privacy, security, web sites.

I. INTRODUCTION

Customers may trust companies based on their privacy policies. In general, privacy policies are norms or established guidelines for the company or institution, with the objective of providing warranty of proper handling of the customer's data.

In early work we evaluated 33 Brazilian electronic commerce sites [1]. We noticed that the majority of them did not have a privacy policy with clear rules and duties, and when they did, they did not use any systematic approach to define them.

The study analyzed if some items, which we considered relevant, were presented by the sites, trying to balance aspects of privacy and personalization. For each site we recorded the items considered, we added specific observations, and summarized the results in a table. We then summarized the advantages and disadvantages that the sites presented to the users, showing the percentages of considered items, percentages of items not considered, and not applicable items. These items were used to define the relevant characteristics that should be considered in a privacy policy.

Turow (2003) discussed privacy policies, emphasizing the dissatisfaction, the lack of understanding and the need for information in existing policies [2]. Another work identified that among 40 privacy policies examined, 12 required a high level of education for understanding them and 7 required the equivalent of a master’s degree level [3]. Another study [4], found similar results for medical sites. Anton [5] surveyed privacy research and indicated the need to make privacy policies more precise. [6] indicates that the policies are usually intended to protect the company from lawsuits and not to apply fair data practices. Her study also showed a wide disparity in the presentation and length of policies (575 to 6135 words), showing a lack of uniformity.

Based on those studies, we concluded that the policies should inform the users about what is being done to guarantee their privacy and which methods are used to provide personalization. The policies should also discuss manipulation of the collected data, use of certification entities, and the security of the stored information.

We present here a set of patterns for the standardization of privacy policies to be displayed in web sites. These patterns attempt to make the policies understandable to the users and include most relevant aspects, highlighted in a written policy, in a clear and objective manner. These patterns consider mostly aspects related to security, privacy, and collection of user information. A pattern is a solution for a problem in a specific context. Patterns have been used effectively for software design [6] and security [7], we believe they are in general valuable to apply good practices and systematize their use.

We define privacy as the right of individuals or groups to keep their personal information away from public knowledge or as their ability to control personal information flow.

In the electronic or the real world, people seek privacy, so they can perform their actions without others monitoring them. Individuals should be able to live without being disturbed and users interacting with the web, navigate without being identified.

When people use the services in the Internet, they leave traces that can be used by companies to record the visited pages, as well as record what was done in each page during the visit, thus building users’ profiles [1]. In this way, the next time that the user visits the site, promotions and recommendations can be presented according to their profiles. While this practice can be useful, it can also bring serious privacy concerns.

While there is a good amount of work on privacy, only a few papers have presented privacy patterns [1, 9]. Two organizations have provided directives for handling personal information: the Organization for Economic Cooperation and Development (OECD)\footnote{http://www.oecd.org}, and the Federal Trade Commision.
The patterns are defined following the hierarchy of Figure 1 where the higher-level patterns use the lower level patterns to refine their concepts. Four abstract levels are used and each pattern is numbered for convenient reference. The first pattern defines a basic need and the lower-level patterns decompose this problem into a set of subproblems. For example, the pattern “Define a Privacy Policy” is considered the main within our group of patterns, and divides a generic problem into a group of subproblems.

In particular, after defining a Privacy Policy we must display it, label it clearly, and place a link to it in a prominent place (end of the page). Having a Privacy Policy implies a set of issues, a notification mechanism to inform users about policy changes, the use of a certification authority, and allowing users to remove themselves from mailing lists or similar.

This paper presents seven patterns that can be used to express in a systematic way a privacy policy. We describe each pattern in detail following the format of [8]. For each one, we show their relevance within the structure of the proposed patterns. At the end of the paper we show an example of a Privacy Policy that uses all these patterns.

II. PATTERN DESCRIPTIONS

A. Pattern 1

Name: PRIVACY POLICY DEFINITION (level 1)

Context: The web is accessed by all kind of users. Personal information is requested in many types of interactions. Preserving the privacy of the users and the security of this information is a fundamental objective.

Problem: In addition to the collection of personal information from the users, web sites may collect additional information, such as their preferences, which also have relevance for their privacy. Not all sites define privacy issues or if they do, they are often not clear or omit important aspects. This means that users do not have a clear picture of what is being done with their information. This, in turn, makes the users mistrust the site. So how can we provide users a way to trust that their privacy will be protected in the systems they are using?

Forces: Without a Privacy Policy the users may feel insecure about what the site will do with their information and they will hesitate about providing their private information. Not explicitly expressing the Privacy Policy followed by a site can also have legal repercussions because of possible lawsuits due to ambiguous or non-existent policies.

Solution: Define a Privacy Policy in a clear and explicit way, informing the users about the rules followed, what the site will do with the collected data, how is this information protected, and what relevant services are offered.

In the development of those policies emphasis should go in: i) usability, to facilitate the use of information and services; ii) accessibility (readability), to allow all users to understand the policies; iii) specific issues about user privacy, to increase their confidence in the site; iv) information about personalization strategies, if they are used with the purpose of minimizing the search time of the users; v) inform about the latest updates of the policies, so users know about any changes and other information relevant to them.

Consequences: Users become more confident when using the services of the site; for example, in the collection of personal information, they are more likely to provide the necessary information.

Besides the user advantages, a Privacy Policy is important to the enterprise, because it may attract more users by offering more security. The enterprise can also improve its own ways to handle personal information and can protect itself better from legal problems. It may be necessary for a site to spend some time understanding the level of language needed by its users to understand the policies.

Known uses: Extra³ and Ponto Frio⁴ are two enterprises in Brazil that offer clear and explicit privacy policies.

Related patterns: Pattern 2 that expands the structure of the general policy.

B. Pattern 2

Name: VISIBLE PRIVACY POLICY (level 2)

Context: We have decided on a privacy policy. We need now a way to make it known to the users in a clear way.

---

2 http://www.ftc.gov

3 http://www.extra.com.br/Institucional

4 http://www.pontofrio.com.br
**Problem:** Many users are not well acquainted with web site structures and don’t know what to expect or where to look for specific aspects. They would give up looking for privacy policies if these are hidden or hard to find. They might not trust the site. When there is no specific place where the Privacy Policy can be found, the users waste time searching for it. This can turn the search for the policies tiresome and frustrating. How do we place the privacy statements on the site so that they are easy to find by the user?

**Forces:** Many sites use different words to identify privacy policies, not worrying about using suggestive words for the users. For example, some of the studied sites used words such as “Security policy”, “Security”, “Buy secure”, and others [1]. Confusing definitions may be seen as a way to make these policies hard to find to avoid their enforcement.

If the user needs to look around for the privacy policy, he might not do it. We need to make this search easy. If the user loses confidence on a site she will not buy from it.

**Solution:** Create a unique name to refer to privacy policies, e.g. “Privacy Policy” and place it in an obvious and easy to find place on the web page. We also need to put a link to it in a well-defined place. The end of the page is a good place for this link.

**Consequences:** Making easier for the user to find the privacy policies of a site increases his confidence and satisfaction in the use of the site. He is able to verify the policy whenever he wants.

**Known Uses:** The sites of Gol Airlines⁵ and Shoptime⁶ uses the name “Política de Privacidade” (Privacy Policy). Companies PontoFrio and Saraiva⁷ place a link to their policies centered on the lower border of the first page.

**Related patterns:** Patterns 3, 4, 5, 6, and 7 define the details of the structure of the policy. Sadicoff et al. show an implementation mechanism using proxies [9].

---

**Pattern 3**

**Name:** PRIVACY POLICY ISSUES (level 3)

**Context:** We have a common and standardized name and a link to the policies. Now we must consider what to include in these policies.

**Problem:** Many sites do not properly handle information about their users and do not inform them about which measures will be taken in case a privacy violation occurs. They do not inform their users about their need to collect personal data either. The users feel may feel threatened and consider navigation of such a site to be unsafe, causing them not to use the available services.

**Forces:** Users need to know the degree of privacy and security offered by a site; otherwise they lose confidence in the site. They also need to know why specific items of information are collected and how are they handled. All the relevant privacy issues should be explicitly and clearly described.

**Solution:** Make it clear in the privacy policies what security measures are used to protect the users’ privacy. The policies should be written in a clear and objective way, warning the users of the possible danger to their privacy during the use of the site. The trustworthiness and veracity of this information should be handled in accordance with the principles established by OECD and FTC.

As an example, Figure 2 shows a display for part of a Privacy Policy. The policy should indicate for example:

**Security:** the site should be responsible for protecting the information collected about the users

**Access:** the users should have access to their collected personal information, could update and delete it

**Choice:** the users should have the option to choose how their personal data can be used

**Transparency:** there should be a general policy that describes all the policies and practices used by the site.

**Related Pattern:** Pattern 2 defines the need to have this information clearly visible.

**Known Uses:** The site Submarino⁸ shows clearly issues about its privacy policy.

---

**Figure 2. Pattern 3 application example**

---

**C. Pattern 4**

**Name:** NOTIFICATION OF RISKS AND CHANGES (level 3)

**Context:** We have a privacy policy, we have defined its contents, and the site has a clear link to it. We now need a way to tell the users of changes to the policies as well as of the possible dangers of using the site.

**Problem:** Some sites define an initial policy and never update it or if they do they don’t inform their users. After a while the users might be relying on a policy that doesn’t exist anymore. When the user provides information she should be warned of possible risks.

**Forces:** Privacy policies need to change due to new legislation, changes in the business, or changes in the financial

---

⁵ http://www.voegol.com.br

⁶ http://www.shoptime.com.br

⁷ http://www.livrariasaraiva.com.br

⁸ http://www.submarino.com.br
or political environment. Sites are able to inform their users of their features through the site itself or by email (they have lists of user addresses).

Keeping the users informed of changes shows a preoccupation with privacy and can increase their confidence on the site.

**Solution:** Notify users of policy changes as soon as a change occurs. The notification can be done through messages displayed in special windows or in a particular place of the policy itself. Using alerting windows is more efficient, since they attract the attention of the users when they are interacting with the site, an alternative is sending email to the users. Place a clause in the Privacy Policy informing users about possible risks and that any alteration in the rules followed by the site will be announced and displayed in the Privacy Policy itself. Figure 3 shows a notification example, in which the site informs the users that they should be careful during their interaction with the web.

**Consequences:** The user knows about the current policies and about the security of the site at all times. This increases her trust in the site.

**Related Patterns:** The Privacy-Aware Network Client Pattern shows how to notify the users of changes in the site [9].

**Known Uses:** The site Submarino, Polishop⁹ and Comprafacil¹⁰ shows issues about the privacy policy. The sites LivrariaCultura¹¹ and Submarino inform their users about the changes in their policies.

---

**Figure 3.** Pattern 4 application example

D. **Pattern 5**

**Name:** PROOF OF SECURITY (level 3)

**Context:** We have deployed our Privacy Policy, it is easy to find, it has the appropriate contents, and it notifies users of changes. We need to prove the degree of our security.

**Problem:** Without some proof of security the user feels insecure, especially when there are transactions involving credit cards. Many sites don’t provide such proofs because of their cost [1].

**Forces:** Users need some reassurance that the site has been certified as secure by some authority; otherwise they need to trust the site’s word.

**Solution:** Get a certificate by some recognized authority attesting about the level of security of the site. The origin and validity period of the certificate must be clearly displayed in the site. The certificate must be signed by the corresponding authority, indicate the URL for which the certification was made, and show a validity period. This is in accordance with the principles established for the OECD, Safety Principle, and FTC, Safety. Figure 4 presents a Privacy Policy that indicates it has been verified by VeriSign, a well-known certifier, describing the security level of the site.

**Consequences:** Users can trust more a site that has been certified by a recognized authority.

**Related Patterns:** This pattern validates the policy defined by pattern 2.

**Known Uses:** The companies Editora Globo¹² and Linux Mall¹³ uses in their sites a certification authority.

---

**Figure 4.** Pattern 5 application example

E. **Pattern 6**

**Name:** PERSONAL INFORMATION OBJECTIVES (level 3)

**Context:** We have an easy to find and complete policy, with appropriate change notification, and the security of the site is certified. Still, the users need to know why do we need to collect specific data from them?

**Problem:** Not all sites are concerned with the user’s knowledge of what is done with the personal data they have collected. This may make users withhold personal information or give false information. Internet users consider it important to know how their personal information is being used [1].

**Forces:** It is important to increase the users’ trust on the site if we want them to provide the information we need to conduct business with them.

**Solution:** Have a section in the Privacy Policy about the collection of data, indicating clearly to the users which data is needed as well as its purpose. Inform the users of the advantages of data collection, as it offers the possibility of personalization that later will facilitate searches and will optimize the available services. Disadvantages should also be described [1]. Figure 5 shows a Policy Privacy with a section about the purpose of the collection of the users’ personal data, including its advantages and disadvantages.

---

¹⁰ http://www.comprafacil.com.br
¹¹ http://www.livrariacultura.com.br
¹² http://editoraglobo.globo.com
¹³ http://www.linuxmall.com.br
**F. Pattern 7**

**Name:** USER CONTROL (level 3)

**Context:** We have a visible policy, our security is certified, and we have the appropriate contents in the policy. We should give some control to the users in case they don’t want to be in our mailing lists.

**Problem:** If sites don’t allow their users to remove themselves from mailing lists, the users will dislike receiving mail they don’t want. They will react by not doing business with the site.

**Forces:** A site keeps mailing lists of its users according to their preferences and it is easy for the site to add or remove users. Users need some control of their interactions with a site because their interests and needs change along time or they might have been wrongly placed in some list. It is annoying to receive unwanted or irrelevant mail.

**Solution:** Allow users to remove themselves from the site’s mailing lists. The site can have options asking users if they want to receive email with special promotions or similar. When the users register in the sites they can choose the reception of e-mails and register their addresses in the lists of promotions, alerts, or novelties. Figure 6 presents to the users the option to receive e-mail about promotions.

**Consequences:** Users are more satisfied when they can select the specific lists that send them advertising or promotions.

**Related Pattern:** This pattern implements one of the requirements of Pattern 2.

**Known Uses:** The sites LinuxMall and VideoLar\(^{15}\) allows the users remove, themselves, their email from the lists.

---

14 http://www.americanas.com.br
15 http://www.videolar.com

---

**III. APPLYING THE PATTERNS TOGETHER**

Table 1 shows an example for a Privacy Policy that combines all the patterns described here. In each pattern instance we applied the requirements discussed earlier and considered the information that should be available for a clear and easy policy.

<table>
<thead>
<tr>
<th>TABLE I. PRIVACY POLICY EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Policy</strong></td>
</tr>
<tr>
<td>Updated in 02/09/2008.</td>
</tr>
</tbody>
</table>

**About this Privacy Policy**

This Privacy Policy was established for the “Example site” with the objective of ensuring the trust and the confidentiality of the information collected about users. We know how important it is for you to know about the use of your personal data. Therefore, we take care to explain and to publish our policies on the use of this information. In this way, you will be better able to understand which information we obtain and how we use it.

**Collected Data**

We request information when you:  
- Register in the website (to expedite the purchase process and for statistical purposes);  
- Place an order;  
- Answer an online survey;  
- Participate in a promotion;  
- Register in our mailing list.

The following data is also automatically collected:  
- E-mail address;  
- Access date and time;  
- Reading time for each page;  
- Sequence of visited pages;

**Registration**

It is not necessary to supply personal information to navigate the site. However, to use some of the services, it will be necessary to identify yourself, and possibly supply some personal data. The information will be stored in a safe server, and it will not be shared with third parties.

**Collection Purpose**

Initially, the collected data will have statistical purposes; for example, to analyze the number of users that read the Privacy Policy, the differences between the privacy preferences of the users, and the frequency of visits to each page. The collected data will also be analyzed to obtain information about the profiles of the users who access the site, so that personalized services can be offered.
We also use the collected information for other statistical purposes, to make purchasing more effective, and for the handling of operations and product shipping.

Data removal
The site makes possible for the users to remove and edit their recorded information, in case they consider this necessary.

Security
All the collected data are stored in secure servers, in a protected database with access restricted to the administrator of this site. In that way, the handling of the data is automatic, with no access for unauthorized persons.

Certification
The practices performed by the site follow the directives defined in these policies and they are certified by a Certification Authority, called XXX, which guarantees our level of security.

To view the security certificate, click here.

Environment for Transactions
We use a secure environment for transactions, encrypting the data, with server authentication, message integrity, and client authentication.

Be careful
It is possible that our pages contain hyperlinks that may take you to other sites. We recommend reading about these sites, since we do not have any responsibility over them. Some people use the trade name of responsible enterprises to send e-mails to the users and also to send executable codes. Do not accept them under any circumstances, because such e-mails or executables may have the purpose to collect your personal information.

Be alert to these e-mails, paying attention to the address of the sender, and, if possible contact us to inform of the occurrence.

Sending of E-mail
This site does not send e-mail with advertisements or promotions without the authorization of the user.

The site provides options that allow users to select the addition or not of their addresses to the mailing lists. Thus, you will be able to cancel the sending of e-mails at any time.

Cookies
Cookies are small text files sent to your computer and stored in the file system. These files serve to recognize, to accompany, and to store the user’s navigation trail in the Internet.

The use of cookies makes possible for the website to offer a more personalized service, in agreement with the characteristics and the interests of the users, making possible offers of contents and publicity specific to the user.

Alterations to this Policy
To assure clear and precise rules, we can eventually modify this policy, and because of this, we recommend its periodic reading. Any alteration in the Privacy Policy will be explicitly shown.

At the beginning of the Privacy Policy the date of the last change is indicated, to facilitate for the user to know when it has been modified.

Final considerations
In case of disagreement about our Privacy Policies or complaints about services performed, feel free to contact:
Fictitious name of enterprise or site
Registered name of CNPJ of the enterprise
Physical address
Phone Support: (XX) XXXX.XXXX at XX:XXhs to XX:XXhs

Electronic Support:
http://www.company.com/support

SUPPORT@COMPANY.COM

IV. CONCLUSIONS

This set of patterns is an effort to improve the expression of privacy policies. As indicated earlier, there is a lack of satisfaction with the way the web sites describe their privacy policies. These patterns can be used to build the needed information and display it in user interfaces. The policy example can be used to guide sites to define their privacy policies. Indirectly, this will benefit the users, since the policies will be defined in clear and objective way, and in a language that the user understands. This will increase user satisfaction and they will feel more secure in interacting with new sites. Clearly, patterns are suggestions or guidelines and they must be tailored to individual situations; for example, different countries may have different regulations about the specific contents of each policy. While there may be other ways to present these patterns, e.g. not using a hierarchy, we believe this is a logical structure to understand their use.

Displaying proper policies is the first step. Our next work will consider ways to enforce the defined policies and audit compliance, two of the problems defined in [5].

ACKNOWLEDGMENT

The work of the first author was supported by the Department of Computer Science of Federal University of São Carlos (UFSCar) and Coordination for the Improvement of Higher Education Personnel (CAPES), Brazil.

REFERENCES


