Towards an Interactive Privacy Pattern Catalog

Olha Drozd
Sabrina Kirrane
Sarah Spiekermann
Vienna University of Economics
and Business
Vienna, Austria
olha.drozd@wu.ac.at
sabrina.kirrane@wu.ac.at
sarah.spiekermann@wu.ac.at

Abstract
A privacy pattern catalog provides guidance with respect to data protection requirements, to both technical and non-technical personnel that are involved in the development of software that processes personally identifiable information. This paper describes a privacy pattern catalog that was compiled with the help of the structured-case methodology. The proposed privacy pattern catalog is an interactive online tool that classifies privacy patterns according to the privacy principle requirements of the ISO/IEC 29100. In addition to the ability to browse through the classification, the tool provides an option to export selected information into a Microsoft Word document for further use. A classification of patterns, based on usage context, application permissions and hierarchical relations of patterns in terms of their level of generality is proposed. While, category, permission and granularity filters are highlighted as a future implementation of the proposed pattern classification scheme.

Author Keywords
Interactive privacy pattern catalog; privacy patterns; privacy by design; privacy principles; ISO/IEC 29100:2011.

ACM Classification Keywords
D.2.11 [Software engineering]: Software architectures — patterns; K.4.1 [Computers and society]: Public policy issues — privacy.

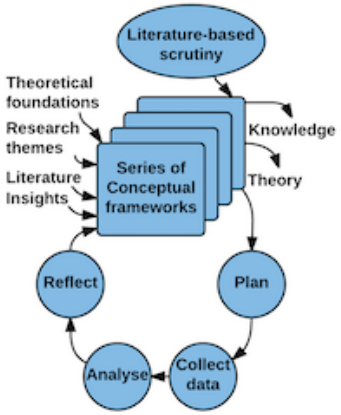

Figure 1: The structured-case research method. (Source: Jenny M. Carroll and Paul A. Swatman. 2000. Structured-case: a methodological framework for building theory in information systems research. European Journal of Information Systems 9, 4 (2000), 235–242)

Introduction

Companies that produce financial, healthcare, insurance, or any other software that processes personally identifiable information (PII) must comply with data protection laws and regulations. In order to do so, software engineers should employ adequate protection mechanisms, which safeguard PII that is processed by their software. This can be achieved by following a Privacy by Design approach, which embeds privacy requirements into both the software architecture and the software design [6]. This paper focuses on the design stage of the software development life-cycle and proposes privacy patterns as tools for the integration of privacy requirements into software artifacts at design time [19]. Patterns are particularly suitable in this context as they offer time-proven solutions to recurring problems in specific contexts [29, 14, 10, 2].

Existing privacy pattern collections [17, 13, 30, 28, 27] provide either privacy patterns for a particular context or an incomplete list of patterns (missing those listed in other sources). Although, a number of projects are interested in accumulating privacy patterns [18, 7], they are still under development and no comprehensive, usable and relatively complete pattern catalog has been put forward to date.

Privacy requirements can be found in data protection laws, regulations and guidelines [8, 25, 26, 9]. However, those differ from country to country, sometimes define the requirements for specific purposes, and often fail to keep pace with technological advancements. The International Organization for Standardization / International Electrotechnical Commission 29100 standard, commonly known as ISO/IEC 29100, is a viable alternative, as its framework aims to protect PII within information and communication technology systems [1]. Moreover, such international standards are prepared in collaboration with international organizations, governmental and non-governmental [1], and, therefore, should ideally cover laws and regulations of different countries. As such, our interactive privacy pattern catalog (IPPC) (*see* the Interactive Privacy Pattern Catalog section for additional details) is a classification of existing patterns according to the privacy principle requirements of the ISO/IEC 29100 standard. Being an interactive online tool, the catalog is available at privacypatterns.wu.ac.at. Building on previous work [12], this paper describes the methodology used to compile the catalog, uses the insights gained in order to propose a classification scheme for privacy patterns, and offers further enhancements to the IPPC.

Method

The structured-case methodological framework for building theory in information systems research [5] was used to collect the content for the IPPC with the help of interviews. The process flow of this method is shown in Figure 1. The *conceptual framework* for the IPPC consists of patterns with their descriptions, privacy principles of the ISO/IEC 29100 and the relationship between them. 13 interviews in 4 *research cycles* were conducted with PhD candidates, PhDs, professors and professionals in the field of data protection from Austria, Germany, Greece, Ireland, Sweden and the USA. As additional insights diminished with each successive interview, the research cycles reached a natural end when no new insights were gained. Although all interviewees were experts in the data protection domain, they had different academic/industry backgrounds and assessed patterns and their descriptions from different points of view. One limitation of the study is the fact that the interviewees felt under time pressure (the interviews lasted up to 4.5 h) and tried to complete the interviews as quickly as possible. Time pressure could potentially be alleviated by splitting interviews into multiple sessions.

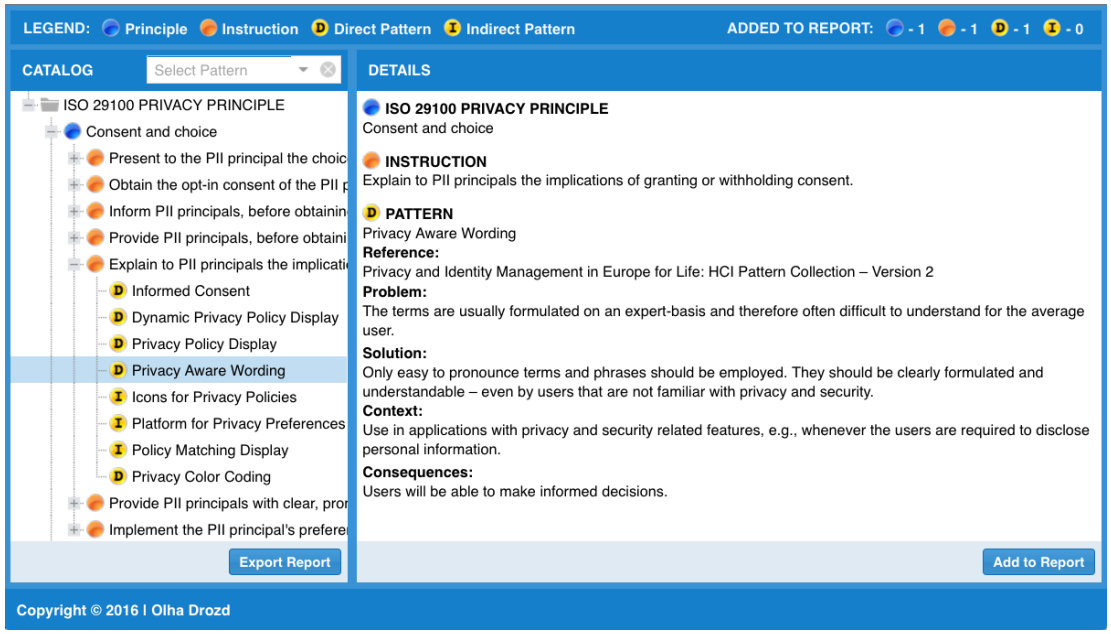

Figure 2: The interactive privacy pattern catalog. (Source:http://privacypatterns.wu.ac.at)

Interactive Privacy Pattern Catalog

The IPPC aims to provide guidance to both software engineers and non-technical personnel with respect to the development and provisioning of privacy aware software systems. However, the catalog can also be used for the training purposes, for example preparation for the ISO/IEC 29100 certification. At the moment this online IPPC contains 40 privacy patterns grouped by privacy principle instructions. Figure 2 shows the catalog and an example of a privacy pattern where a pattern belongs to an instruction which in turn belongs to an ISO privacy principle. The full hierarchy, patterns and their descriptions are available in the online IPPC [11]. In addition to just browsing through the catalog, users can search the contents of the catalog by privacy pattern and export the information they selected into a Microsoft Word document. This export serves as a privacy instruction catalog that is specifically targeted to the end users requirements.

Challenges and Opportunities

While compiling the catalog we uncovered a number of open challenges and opportunities, with respect to the usability of privacy design patterns, that still need to be addressed. Specifically, the need for the further classification

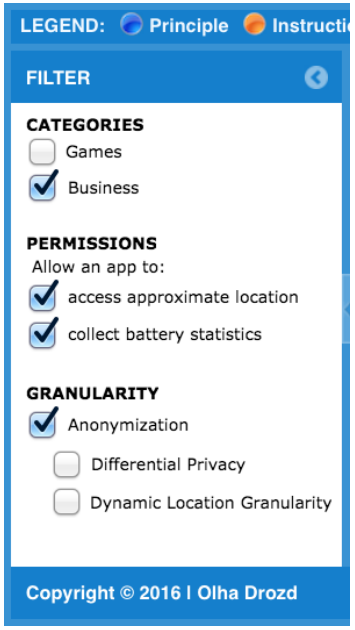

Figure 3: The prototype of the 'Filter' sidebar.

of patterns based on usage context, application permissions and hierarchical relations between patterns in terms of their level of generality. In the next release of the IPPC such a scheme will be realized in the form of category, permission and granularity filters, that could be used to browse the privacy pattern catalog (*see* Figure 3).

When reading the description of a pattern, interviewees often mentioned that a pattern can be directly or indirectly connected to the privacy principle requirement of the ISO/IEC 29100 standard depending on the context where the pattern is applied. To disambiguate the context of pattern usage, additional privacy pattern classifications are needed. A possible approach for context filtering is to use general software classifications based on context. However, such classifications [15] appear to be too general and sometimes all patterns can be fitted to every category. Another approach is to use software classification on a lower level in the classification hierarchy. Mobile appstores [24, 16, 20] offer a comprehensive and more detailed context grouping of applications (i.e. apps). A 'categories' filter could be used by non-technical personnel, for example managers, chief executive officers, etc., to obtain a general idea of what might be required for their applications, in terms of privacy.

Software engineers, however, may require a more detailed context filter, which is even lower in the classification hierarchy in comparison with app categories. This filter could be based on the permissions required by the software application. The 'permissions' filter could be used to identify possible privacy-friendly solutions, in terms of design patterns, for the processing of PII. Three of the most popular operating systems (Android, iOS, and Windows), were taken into account when compiling the list of permissions. Those operating systems (OSs), according to Böhm et al., hold 84.4%, 11.7% and 2.9% of the market share respectively and constitute 99% of the global market share [4]. Permissions for Android are clearly listed on the official website [3] for the Android developers. Apple, however, does not offer an official source that explicitly lists permissions and no papers with the analysis of permissions for the iOS were found. Nevertheless, permissions can be retrieved from the iOS developer library [21] as well as from the 'privacy settings' section of Apple mobile devices. Microsoft provides a list of potential app permissions on their official website in the Windows Dev Center section [22], on the official website for Windows Phone OS [23] as well as in the privacy tab in the settings menu of the OS itself.

Finally, the interviewees identified an issue with the different levels of pattern generality. For example, anonymity and differential privacy are listed as separate patterns in the catalog, although the differential privacy pattern may be considered as a part of the anonymity pattern. To solve this problem, it is necessary to introduce a hierarchy of macro- and micropatterns, group patterns accordingly and add a corresponding filter to the catalog. Such a structure could be defined based on existing privacy taxonomies, standardization activities and engineering practices.

Conclusion

This paper described an interactive privacy pattern catalog that can be used by both technical and non-technical personnel in order to obtain guidance with respect to the processing of personally identifiable information. Further, we discussed the challenges that arose during the compilation of the catalog and identified the need for the further classification of patterns based on usage context, application permissions and hierarchical relations between patterns in terms of their level of generality. Finally, we proposed the realization of a more usable privacy catalog in the form of category, permission and granularity filters.

REFERENCES

1. ISO/IEC 29100:2011. 2011. Information technology - Security techniques - Privacy framework. (2011).
2. Christopher Alexander, Sara Ishikawa, and Murray Silverstein. 1977. *A Pattern Language: Towns, Buildings, Construction*. Vol. 2. Oxford University Press. 1171 pages.
3. Android. 2016. Developers. (2016). https://developer.android.com/reference/android/Manifest.permission.html.
4. Stephan Böhm, Fabian Adam, and Wendy Colleen Farrell. 2015. Impact of the Mobile Operating System on Smartphone Buying Decisions: A Conjoint-Based Empirical Analysis. In *Mobile Web and Intelligent Information Systems*. Springer, 198–210.
5. Jenny M. Carroll and Paul A. Swatman. 2000. Structured-case: a methodological framework for building theory in information systems research. *European Journal of Information Systems* 9, 4 (2000), 235–242.
6. Ann Cavoukian. 2011. Privacy by Design. The 7 Foundational Principles. (2011). https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.
7. International collaboration. 2015. Privacy Patterns. (2015). https://privacypatterns.eu.
8. Federal Trade Commission and others. 2000. Privacy Online: Fair information practices in the electronic marketplace: A report to congress. *Federal Trade Commission* (2000).
9. The European Commission and the U.S. Department of Commerce. 2016. EU-U.S. Privacy Shield. (2016). http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm.
10. James O. Coplien. 2000. *Software Patterns*. Lucent Technologies, Bell Labs Innovations, New York.
11. Olha Drozd. 2016. Privacy Pattern Catalog. (2016). http://privacypatterns.wu.ac.at.
12. Olha Drozd. To appear. Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process. In *Time for a revolution?* Springer. https://www.wu.ac.at/fileadmin/wu/d/i/ec/Research/PPC.pdf.
13. Simone Fischer-Hübner, Christina Köffel, John-Sören Pettersson, Peter Wolkerstorfer, Cornelia Graf, Leif Erik Holtz, Ulrich König, Hans Hedbom, and Benjamin Kellermann. 2010. HCI Pattern Collection - Version 2. (2010), 61.
14. Erich Gamma, Richard Helm, Ralph E. Johnson, and John Vlissides. 1995. *Design patterns. Elements of reusable object-oriented software*. Addison-Wesley. 395 pages.
15. Robert L. Glass and Iris Vessey. 1995. Contemporary application-domain taxonomies. *IEEE Software* 12, 4 (1995), 63.
16. Google. 2016. Google Play. (2016). https://play.google.com/Store.
17. Munawar Hafiz. 2006. A collection of privacy design patterns. In *Proceedings of the 2006 conference on Pattern languages of programs*. ACM, 13.
18. Jaap-Henk Hoepman. 2014a. Patterns for Privacy (P4P). (2014). http://www.cs.ru.nl/~jhh/p4p/proposal.pdf.

19. Jaap-Henk Hoepman. 2014b. Privacy design strategies. In *ICT systems security and privacy protection*. Springer, 446–459.

20. Apple Inc. 2016a. App Store. (2016). https://itunes.apple.com/at/genre/ios/id36?mt=8.

21. Apple Inc. 2016b. iOS Developer Library. iOS Keys. (2016). https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Articles/iPhoneOSKeys.html.

22. Microsoft. 2016a. Windows Dev Center. (2016). https://msdn.microsoft.com/en-us/library/windows/apps/jj206936(v=vs.105).aspx.

23. Microsoft. 2016b. Windows Phone. (2016). https://developer.android.com/reference/android/Manifest.permission.html.

24. Microsoft. 2016c. Windows Store. (2016). https://www.microsoft.com/en-us/store/apps.

25. OECD. 1980. OECD guidelines governing the protection of privacy and transborder flows of personal data. (1980).

26. The European Parliament and the Council. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

27. Siani Pearson and Yun Shen. 2010. Context-aware privacy design pattern selection. In *Trust, Privacy and Security in Digital Business*, Vol. 6264. Springer, 69–80.

28. PRIPARE. 2015. Privacy Pattern Portal. (2015). http://pripareproject.eu/.

29. Douglas C. Schmidt and Frank Buschmann. 2003. Patterns, frameworks, and middleware: their synergistic relationships. In *25th International Conference on Software Engineering, 2003. Proceedings.* IEEE, 694–704.

30. UC Berkeley School of Information. 2016. Privacy Patterns. (2016). http://privacypatterns.org/.