LPL Personal Privacy Policy User Interface: Design and Evaluation

Armin Gerl[1], Florian Prey[2]

Distributed Multimedia Information Systems (DIMIS), University of Passau[1]
Faculty of Computer Science and Mathematics, University of Passau[2]

armin.gerl@uni-passau.de, prey01@fim.uni-passau.de

Abstracts

We present the LPL Personal Privacy Policy User Interface (LPL PPP UI), which is intended to inform Data Subjects about the contents of the privacy policy and to allow personalisation of purposes to support free and informed consent. The capabilities of the LPL PPP UI, consisting in informing the Data Subject about the contents of a privacy policy in a structured way and personal privacy interactions are presented. The LPL PPP UI is evaluated against regular designed privacy policies. Furthermore, future challenges and objectives for privacy policy user interfaces are given.

1. Motivation

The *Layered Privacy Language (LPL)* represents privacy policies that allow the expression and enforcement of privacy properties such as personal privacy, user consent, data provenance, and retention management (Gerl et al., 2018). It is intended to allow *Data Subjects* to accept and consent to privacy policies and enforce privacy-preserving processing based upon the consented personalised privacy policy. Therefore, the privacy process 'from consent to processing' is represented. To allow a *Data Subject* to consent to a privacy policy as well as personalisation of the LPL Personal Privacy Policy UI is presented and evaluated.

The *General Data Protection Regulation (GDPR)* entered into force on 25th May and is designed to standardise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to rework the way organisations approach data privacy. In general, the GDPR specifies that consent has to be given freely, specific, informed and unambiguous (Council of the European Union, 2016, Art. 4 No. 11). Additionally, the concept of *Personal Privacy* (Xiao & Tao, 2006) is considered. It states that the user can influence the privacy properties of the processing.

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Workshopband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-ws08-0540

It is shown that privacy policies are hard to understand and often not read (Ermakova et al., 2015; Obar and Oeldorf-Hirsch, 2016). Especially the understanding of the content of the privacy policies often varies between the Data Subject and the privacy experts, which create them, which can lead to significant misunderstandings (Reidenberg et al., 2015). This leads to missing trust in the processing of personal data (Symantec, 2015). Several pitfalls for the creation of privacy policy user interfaces have been identified, consisting of obscuring potential information flow, obscuring actual flow, emphasizing configuration over action, lacking coarse-grained control, and inhibiting established practice (Lederer et al., 2004). Therefore, guidelines for the creation of usable privacy policies have been proposed to allow transparency (Waldman, 2016; Renaud and Shepherd, 2018).

In the literature, several user interfaces have been developed based on a privacy language supporting the *Data Subject*. For example for *P3P* the *'AT&T Privacy Bird'* browser plugin (Crano et al., 2002), privacy policy visualisations (W. Reeder, 2008; W. Reeder et al., 2008), as well as a *'Nutrition Label'* (Kelley et al., 2010; Kelley et al., 2009) have been proposed. *For Primelife Policy Language (PPL)* the *'Send Data?'* browser extension has been developed (Angulo et al., 2011). Each visualisation or user interface, with their respective privacy language, considers different aspects to improve the perception of privacy policies for the *Data Subject*.

Also other works, which are not based on a privacy language, aim to improve privacy policies. For example the introduction of contextual privacy statements (Feth, 2017), a *privacyTracker* framework allowing data traceability (Gjermundrød et al., 2016), and a privacy dashboard to pursue *Data Subject Rights* (Raschke et al., 2018) have been proposed.

Although several attempts have been made to improve privacy policies, current state-of-the-art privacy policies are usually purely text-based and only allow two options – consent or dissent. It is debatable whether such privacy policies really inform the users about the processing of their data. Therefore, we introduce a user interface based on LPL, with the intention both to allow free and informed consent as well as personalisation as required by the newly-enforced GDPR.

The main contributions of this paper are the presentation of the LPL Personal Privacy Policy UI based upon *the Layered Privacy Language*, as well as the *Privacy Policy Comparison Evaluation* evaluating the LPL Personal Privacy Policy UI against a regular privacy policy representation. Hereby, we define a regular privacy policy on a natural-language text-based unstructured privacy policy, which might be formatted and highlighted with e.g. different text styles or colors.

The remaining of the paper is structured as follows: Section 2 describes the LPL Personal Privacy Policy UI, which will be evaluated in section 3. Lastly, section 4 concludes the paper and provides an outlook for future works.

2. LPL Personal Privacy Policy UI

The LPL Personal Privacy Policy User Interface (LPL PPP UI) is structured in three main parts – *Policy Header*, *Purpose Overview* and *Purpose Details* (see Figure 2). The user interface is based on the structure of the *User Interface Extension* (Gerl, 2018) of LPL (Gerl et al., 2018). The overall design follows principles of the *Visual Information Seeking Mantra*, with an emphasis on *Overview*, *Filter* and *Details on Demand* (Shneiderman, 1996) to provide the Data Subject with both an overview and details of the content of the privacy policy.

LPL is a privacy language models a privacy policy with the *LayeredPrivacyPolicy-element* as its root element. The main structure of the privacy policy is furthermore defined by a set of Purpose-elements, which moreover contains a set of *DataRecipient-elements*, set of *Data-elements*, set of *PrivacyModel-elements* as well as a *Retention-element*. The Purpose- and Data-element both contain an attribute required defining if they can be consented or dissented to. The set of *Icon-elements* is introduced to support the *Privacy Icon Overview* (Gerl, 2018). All of the mentioned elements so far inherit from the *UIElement* to support human-readable headers and descriptions. *The AnonymizationMethod-element* and the *PrivacyModel-element* enable policy-based anonymization that takes into account the personal data and the personalized privacy policies that have been consented to by the individual Data Subjects (Gerl et al., 2018). The detailing of further elements and attributes is omitted for the scope of this paper.

The LPL PPP UI is based on the structure of LPL but not LPL itself. A similar privacy language to LPL could be developed or LPL could be extended in a way that the visualization concepts of the in the following described LPL PPP UI are still applicable.

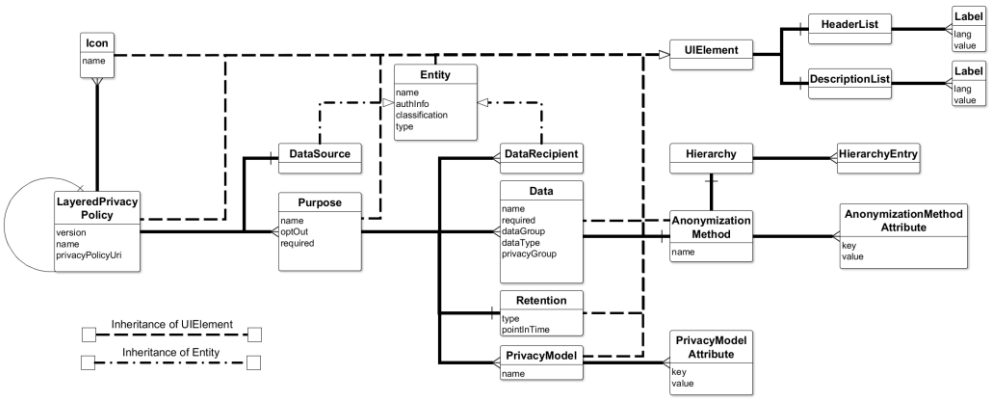

Figure 1: Elements and Strucutre of LPL with the User Interface Extension.

Based on the web-browser settings the localisation of the user interface as well as the LPL privacy policy is selected and displayed, allowing the support of several localisations with a common machine-readable privacy policy definition.

The *Policy Header* not only represents the title of the policy, but also provides a link to the regular textual representation of the privacy policy to comply with the current standards. Furthermore, a *Privacy Icon Overview* is giving an overview over the processing of the personal data allowing the Data Subject to identify purposes better (Gerl, 2018). Note that the shown icons should be seen as a placeholder until a standardised icon set (Council of the European Union, 2016, Art. 12 No. 7) has been defined.

The *Purpose Overview* lists all purposes of the privacy policy and offers the *Data Subject* two interactions. On the one hand, it allows the *Data Subject*, if specified by the creator of the privacy policy, to accept/deny the purpose and therefore to personalise the privacy policy. On the other hand, it allows the *Data Subject* to select (*Filter*) a purpose updating the displayed information in the *Purpose Details* (*Details on Demand*).

The *Purpose Details* represents the specific content or regulation of the selected purpose, giving details about purpose including the data, data recipient, retention, and anonymisation. The title and description of the purpose are given. Further details will not be shown and require an interaction (click on the purpose entry) to be displayed, minimising the by default displayed information.

The data is listed similar to the *Purpose Overview* and *Purpose Details*. All data is listed for the selected purpose, whereas the selection of a data displays further details about it including a title, description and how it is anonymised. As no personal data can be legally processed before the privacy policy is accepted, unless there is a legal basis (Council of the European Union, 2016, Art. 6), the anonymisation will be shown by a default example. The recipients are also displayed as a list from which a single recipient can be selected for additional details. For the retention the date for the deletion of the data will be displayed. As the date is not always defined uniquely in LPL, the displayed date will be generated based on the underlying LPL element *Retention*. This element can define a fixed date, a time frame after the fulfilment of the purpose or indefinite retention. Lastly, the anonymisation of the overall data can be displayed, which is defined by privacy models like *k-Anonymity* (Sweeny, 2002) or *l-Diversity* (Machanavajjhala et al., 2007). For a better understanding, the risk of identification (calculated from the configuration of the privacy model) is displayed, as privacy models would require expert knowledge to be understood; that is not given for regular users.

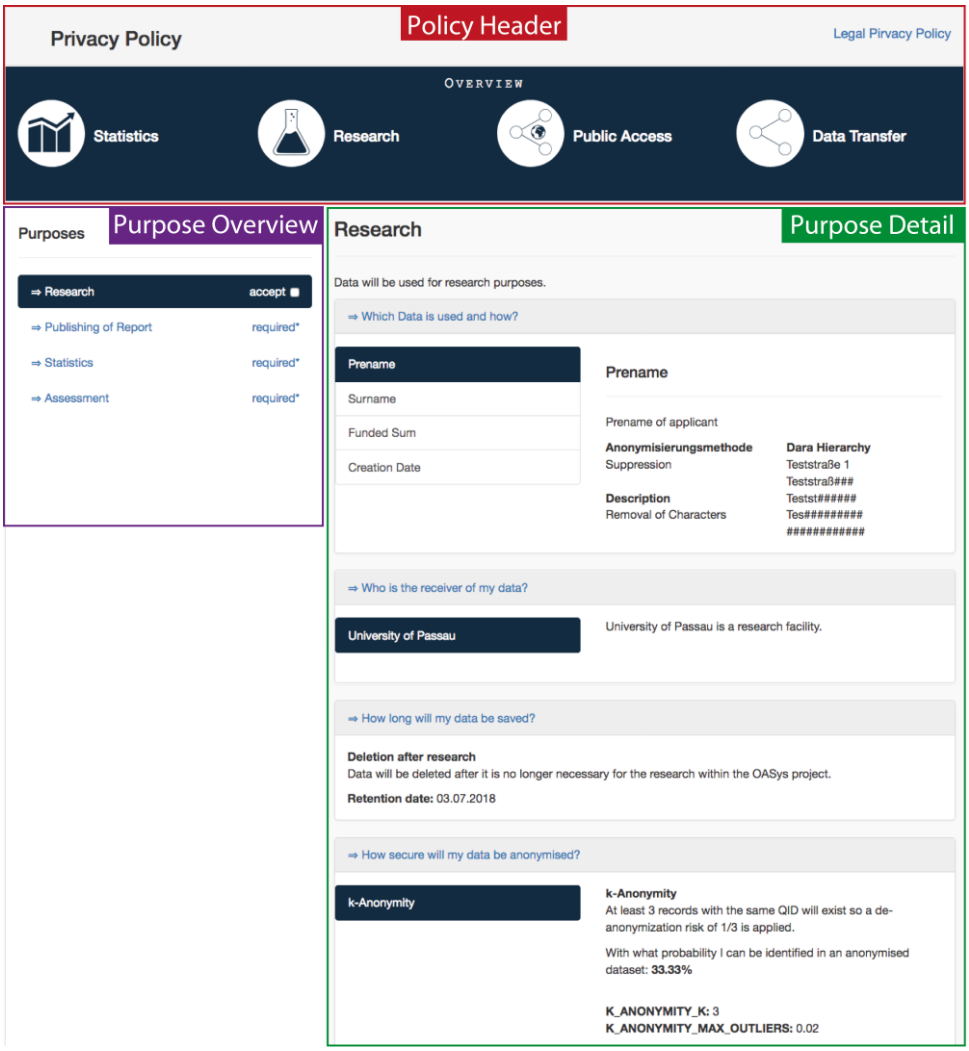

Figure 2: LPL Personal Privacy Policy User Interface with example privacy policy. The Policy Header, Purpose Overview and Purpose Detail components are highlighted.

The remaining design principles have been excluded for the scope of this prototype but possible implementation is discussed in the following. *View Relationships* could visualise how data fields are used within automatic decision-making (Council of the European Union, 2016, Art. 13 No. 2). A *History* of accepted privacy policies could be made available for the *Data Subject* to reflect its decisions, which would also require *the Data Subject* to *Extract* the privacy policy contents.

3. Privacy Policy Comparison Evaluation

We evaluated our LPL PPP UI prototype against a regular privacy policy with the goal to determine if the LPL PPP UI has benefits for the Data Subject. Hereby, both the average time spent on the privacy policy view as well as a score, which represents correctly answered questions about the privacy policy, are considered.

3.1. Experiment Design

We designed four tasks for the *Privacy Policy Comparison Evaluation*. Two tasks (task 1 and 2) have been designed so that the user has to find specific information from the given privacy policy, and provide the answer. The other two tasks (task 3 and 4) have been designed, so that the user has to inform him in general about the privacy policy. For each task group the first task used a less complex privacy policy than the second one. After each task a questionnaire had to be answered. Each correctly answered question scored a point.

In the experiment, twelve random volunteers participated, separated in two groups (A and B). Group A had four female and two male participants. Group B had three female and three male participants. Each group had to fulfil four tasks. The volunteers use the internet regularly. The participants have not been educated about the LPL PPP UI beforehand and have not been involved in the development.

The tasks have been presented alternating with a regular and a LPL privacy policy. If group A was presented the task with a regular privacy policy then group B was presented the task with a LPL privacy policy. Therefore, each group had to fulfil two tasks with a regular and two tasks with a LPL privacy policy. For each task, the average time that the participants spent on the privacy policy view has been measured. For example in the first task the user had to determine the date for the retention. In the second task the participants had to determine the receivers of their personal data. Additionally, an average score has been measured based on correctly answered questions in each of the follow up questionnaires. No introduction or training for the LPL PPP UI has been given.

3.2. Results

The results of the evaluation are shown in Table 1. It can be observed that task 1 could be solved correctly from all users, who were presented with the regular privacy policy. One user, presented the LPL PPP UI, was unable to solve the task correctly, which lead to a score of 83%. After a review of the answers, we assume that this was the result of a typographical error.

The score of task 3 is higher for LPL PPP UI. This cannot be observed for task 4, where the score for LPL PPP UI is less than for the regular privacy policy. Comparing the average time measurements of task 1 and 2 of the LPL PPP UI and regular privacy policy, it can be observed that after the first presentation of LPL PPP UI in task 1 for group A and respectively task 2 for group B, in which more time was required for the LPL PPP UI version compared to the regular privacy policy, less time was required for it in task 3 for group A and task 4 for group B.

For task 3 and 4, when the participants are confronted with a LPL privacy policy for the second time, it can be observed that the average time required is always less compared to the regular privacy policy. Comparing the average time of the different task types (task 1 and 2 with task 3 and 4) it can be observed that the search for specific information requires less time on average compared to the task to inform themselves in general about the privacy policy.

Tasks 3 and 4 now correspond to more extensive data protection declarations. In task 3, the expected result has occurred on the basis of the hypothesis. The time required here with LPL PPP UI is less than the textual counterpart, but the score is higher, albeit only slightly. In task 4, a similar time factor can be examined as in task 3, but the score is higher for the text-based privacy policy representation.

Task (Group)	**LPL Personal Privacy Policy UI**		**Regular Privacy Policy**	
	Time (s)	***Score (%)***	***Time (s)***	***Score (%)***
1 (A/B)	12,78	83	12,31	100
2 (B/A)	17,30	50	14,81	39
3 (A/B)	22,43	98	32,33	88
4 (B/A)	34,48	68	40,63	72

Table 1: Mean quantitative results of the Privacy Policy Comparison Evaluation are shown. Average time is measured in seconds (s) and the score is percentual to the maximum score. Tasks are differentiated according to the usage of the LPL Personal Privacy

3.3. Interpretation

We interpret the results as follows. Only the results of task 3 matched our expectations for which the LPL PPP UI caused the user to spend less time on the privacy policy view, while having a higher score. The results of group A, with the LPL PPP UI, have been better both in terms of the average score and the required time, compared to group B.

After the initial usage of the LPL PPP UI in task 1 for group A and task 2 for group B, it can be observed that the average time measured for LPL PPP UI has always been lower than for the regular privacy policy. This lets us assume that the participants had a learning effect after the initial usage of the LPL PPP UI.

The difference in the average score values, considering the amount of participants, seems not to be large enough to conclude that either the regular privacy policy or the LPL PPP UI can inform the user significantly better. Rather, it can be stated that the LPL PPP UI has a similar effectiveness to a regular textual representation of a privacy policy.

According to our results, we conclude that no significant advantage of LPL PPP UI over regular privacy policies can be shown. Concurrently, no significant disadvantages over regular privacy policies can be shown. The average time spent on the personal privacy view decreased

after an initial use of the LPL PPP UI, which is promising. But the inconsistent results on the average score achieved for both the LPL PPP UI and regular privacy policies have to be further inspected requiring additional extended evaluations. We interpret the results to be promising overall, but also acknowledge the need for extended evaluations with more participants to improve the reliability and significance of the evaluation.

4. Conclusion and Future Works

Based on the *Layered Privacy Language (LPL)* this paper introduces the *LPL Personal Privacy Policy User Interface (LPL PPP UI)* as an alternative representation for privacy policies supporting a free and informed consent. Furthermore, the LPL PPP UI was evaluated against the regular text-based privacy policy representation. Although the evaluation showed inconclusive results whether the LPL PPP UI has benefits over regular privacy policy representations due to its limited extent, the evaluation showed similar results for both the time spent on the privacy policy view as well as the achieved score. After the evaluation the participants have been asked about their subjective perception on the new way of presentation of a privacy policy. The participants answered overall positive supporting the idea of having privacy policies which are not only text-based. Overall it is shown that the LPL PP UI is a viable proof-of-concept for a privacy policy representation based on LPL.

The Layered Privacy Language (LPL), an overarching privacy framework, and the presented *LPL Personal Privacy Policy User Interface (LPL PPP UI*), which is implemented as a jQuery library, are elements in ongoing work. Further research has to be conducted for which an outlook will be provided in the following.

The presented version of LPL PPP UI solely supports personalisation based on the consent/dissent of purposes. Following the presented principle, the personalisation of the processed data, recipients as well as the degree of anonymisation will be integrated in the LPL PPP UI allowing a fine-grained control over the processed personal data for the *Data Subject*. Accordingly, extended evaluations of the LPL PPP UI are required.

The machine-readability of LPL facilitates further possibilities to support the Data Subject in the decision-making regarding its own privacy. The definition of personal privacy preferences would allow the automatic comparison against presented privacy policies of e.g. a web-service informing the *Data Subject* about the compliance, determining matches and conflicts, to its personal privacy preferences. This could be further extended to apply personal privacy preferences on the presented privacy policy to ease its personalisation.

Furthermore, different user groups with special requirements, e.g. children, have to be taken into account and require possible specialised variations of LPL PPP UI. Additionally, the provision of LPL PPP UI implementation for different use-cases, e.g. programming languages or content-management systems (CMS), is required for a broad and viable adoption.

References

Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E. (2011) *Towards Usable Privacy Policy Display & Management for PrimeLife*. In 5th International Symposium on Human Aspects of Information Security and Assurance (HAISA). London:University of Plymouth. Pages 108–118.

Crano, L. F., Arjula, M., Gudrun, P. (2002) *Use of a P3P user agent by early adopters.* In Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society. New York: ACM. Pages 1-10.

Council of the European Union. Council of the European Union. General data protection regulation, April 2016. *Regulation (EU) 2016 of the European Parliament and of the Council of 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.*

Ermakova, T., Fabian, B., & Babina, E. (2015). Readability of Privacy Policies of Healthcare Websites. In Wirtschaftsinformatik (pp. 1085-1099).

Feth, D. (2017). Transparency through Contextual Privacy Statements. Mensch und Computer 2017-Workshopband: Spielend einfach interagieren, 13, 289.

Gerl A. (2018). *Extending Layered Privacy Language to support Privacy Icons for a Personal Privacy Policy User Interface.In Proceedings of Brithish HCI 2018. Belfast:BCS Learning and Develoment Ltd.*

Gerl A., Bennani N., Kosch H., Brunie L., (2018) *LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage. In LNCS Transactions on Large-Scale Data- and Knowledge-Centered Systems*, XXXVII, The final authenticated publication will be available online on SpringerLink, https://link.springer.com/

Gjermundrød H., Dionysiou I., Costa K. (2016) privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls.

Kelley, P.G., Bresee, J., Cranor, L.F., W. Reeder, R. (2009) *A "nutrition label" for privacy.* In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS). New York: ACM. Pages 4:1-4:12.

Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F. (2010) *Standardizing privacy notices: an online study of the nutrition label approach*. In Proceedings of the 28th International Conference on Human Factors in Computing Systems. New York: ACM. Pages 1573-1582.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: five pitfalls for designers. Personal and Ubiquitous Computing, 8(6), 440-454.

Machanavajjhala A., Kifer D., Gehrke J., and Venkitasubramaniam M. (2007), *L-diversity: Privacy beyond k-anonymity*. ACM Trans. Knowl. Discov. Data, 1(1).

Obar, J. A., Oeldorf-Hirsch, A. (2016). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services.

Raschke P., Küpper A., Drozd O., Kirrane S. (2018) Designing a GDPR-Compliant and Usable Privacy Dashboard.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30, 39.

Renaud, K., Shepherd, L. A. (2018). How to Make Privacy Policies both GDPR-Compliant and Usable.

Shneiderman B. (1996), *The eyes have it: A task by data type taxonomy for information visualizations*. Technical report, Department of Computer Science, Human-Computer Interaction Laboratory, and Institute for Systems Research, University of Maryland.

Sweeney, L. (2002) *k-Anonymity: A Model for Protecting Privacy*. In International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10, pages 557–570.

Symantec. State of Privacy Report 2015.

Waldman, A. E. (2016). Privacy, Notice, and Design.

W. Reeder, R. (2008) *Expandable Grids: A user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring*. School of Computer Science Carnegie Mellon University Pittsburgh, Pennsylvania, USA.

Xiao, X. and Tao, Y. (2006) *Personalized privacy preservation*. In ACM SIGMOD International Conference on Management of Data. New York: ACM. Pages 229–240.

Authors

Gerl, Armin

Armin Gerl is a Cotutelle PhD student between University of Passau (Germany) and INSA Lyon (France). The goal of his thesis is to create the Layered Privacy Language (LPL) that considers both the legal view (General Data Protection Regulation) and technical view (Privacy Preservation, Anonymization, Privacy Models etc.). Based on LPL, an overarching privacy framework is developed to ensure privacy ‘from consent to processing’. Therefore, he is interested in everything related to privacy especially from different point of views.

Florian, Prey

Florian Prey is a Master Student at the University of Passau and also works as Software Developer at ONELOGIC GmbH also in Passau. His Master Thesis focused on create a user interface for the Layered Privacy Policy together with a research on how user think about privacy in the world wide web and also how to improve privacy policies and make it more understandable to the user.