A Literature Study on Privacy Patterns Research

Jörg Lenhard, Lothar Fritsch, and Sebastian Herold
Department of Mathematics and Computer Science
Karlstad University
651 88 Karlstad, Sweden
Email: {joerg.lenhard, lothar.fritsch, sebastian.herold}@kau.se

***Abstract*—*Context:* Facing the implementation of the EU General Data Protection Regulation in May 2018, many commercial software providers will soon need to adapt their products to new privacy-related constraints. Privacy patterns defined for different aspects of the software engineering process promise to be a useful concept for this task. In this situation, it seems valuable to characterize the state of the research related to privacy patterns.**

***Objective:* To identify, characterize and classify the contributions made by published research results related to patterns in the context of considering privacy concerns in engineering software.**

***Method:* A literature review in form of a mapping study of scientific articles was performed. The resulting map structures the relevant body of work into multiple dimensions, illustrating research focuses and gaps.**

***Results:* Results show that empirical evidence in this field is scarce and that holistic approaches to engineering privacy into software based on patterns are lacking. This potentially hinders industrial adoption.**

***Conclusion:* Based on these results, we recommend to empirically validate existing privacy patterns, to consolidate them in pattern catalogues and languages, and to move towards seamless approaches from engineering privacy requirements to implementation.**

I. Motivation

The General Data Protection Regulation (GDPR) will come into effect in the European Union in May 2018 [1]. This regulation has the goal to harmonize data protection in the EU and to strengthen the data protection rights of individuals across Europe. It also includes sizable penalties, of up to 4% of the annual global turnover, for enterprises that fail to comply with the regulation. In order to achieve compliance with the GDPR, many IT system providers, particularly software-producing enterprises, will need to adapt their systems. This is expected to cause massive efforts [2]. Hence, equipping software engineers in industry with effective and systematic approaches for engineering privacy and data protection requirements into software is a crucial and valuable area of research.

A few propositions have been made on how to integrate privacy concerns into the software engineering process. One approach, called *Privacy by Design* (PbD), aims at ensuring that systems conform to privacy regulations, directing particular attention to a correct translation from legal requirements into technological solutions [3], [4]. *Privacy (design) patterns* have been suggested as a central building block for this translation [5]. Nevertheless, PbD falls short of defining concrete privacy patterns or outlining essential characteristics of such patterns.

Patterns have been extensively researched by the software engineering community and have been collected in catalogues for different subfields [6], [7], [8]. Similar catalogues have also been developed for several technical aspects of software systems that are related to the field of privacy, such as security [9], [10]. Several large-scale research projects focus on privacy technology, privacy engineering, and the application of privacy technology, such as SEMPER [11], PRIME [12], PRIMELife [13], or FutureID [14], and researchers recently started investigating privacy design patterns. Joint effort has lead to collections of patterns such as *privacypatterns.org* [15] and *privacypatterns.eu* [16]. Compared to other areas, however, privacy patterns are a relatively young field.

In this present situation—the relatively young but maturing field of privacy patterns opposed to the urgent need for systematic approaches to engineering privacy in the light of the GDPR—it seems worthwhile to review the current state of the research field in order to identify research focuses and gaps as well potential implications for practical applications. This motivates the research question of this study: *What is the state of empirical evidence regarding the relevance, occurrence and use of privacy patterns?*

To address these questions, we performed a systematic mapping study of peer-reviewed scientific publications on patterns for privacy in engineering software [17]. Four major databases of scientific publications were searched for relevant articles, followed by a snowballing phase. Relevant articles were categorized and systematically sorted into a map. Privacy patterns proposed in the relevant articles were extracted and categorized for a more fine-grained analysis regarding supported software activities and privacy strategies.

The remainder of the paper is structured as follows: Sec. II presents the protocol followed in this mapping study. In Sec. III, the results of mapping articles and patterns are presented. The results are discussed and interpreted in Sec. IV. Sec. V outlines related work, followed by concluding remarks in Sec. VI.

II. Study design

The mapping study's design follows the process for this type of literature study suggested by Petersen et al. [17]. The original process consists of the subsequent steps of defining the research questions, conducting the search for research articles, the screening of articles for relevance, the keywording of relevant articles, and the data extraction and mapping. Each of the following subsections covers one of these process steps,

except for the definition of the research question of the study which has already been presented in Sec. I.

A. Conducting the Search

The initial set of primary studies were retrieved through querying four large databases of scientific publications, namely Scopus, ACM Digital Library, IEEExplore, and SpringerLink. The search strings applied were expressions in conjunctive normal form consisting of three disjunctive terms. The literals in each term were names of concepts or phrases covering three different aspects that potentially relevant articles should address. First, relevant articles should address "privacy" or "data protection"; second, relevant articles should refer to "pattern" or other concepts that could be interpreted as patterns, such as "best practice", "anti-pattern", "smell", "abstract solution", "reusable solution", or "repeatable solution"; third, relevant articles should refer to "software engineering", "software development", "software design", "software architecture" or "software technology". The concrete search strings were adapted to the single database's query language syntax and accordingly extended by wildcards to also detect inflections of the terms used. This initial search step returned 480 articles.

After the screening of articles (see Sec. II-B), we applied backward and forward snowballing based on the articles considered relevant for the study [18]. For backward snowballing we focused on references in articles from the initial set of articles that were listed in their related work sections or that were explicitly mentioned as "pattern containing" in introducing sections. Forward snowballing was applied using the articles' "Cited by" data available in Google Scholar.

B. Screening of Articles

The articles retrieved from the databases and from snowballing were screened for relevance based on several inclusion and exclusion criteria. Articles published via peer-reviewed channels were included whereas slide presentations, keynote abstracts, forewords, and publicly available project deliverables were excluded if it was not clear whether they had been peer-reviewed by the research community. The main content-related inclusion criterion was that the title, the abstract, or the associated keywords must mention privacy and patterns (or one of the synonyms described in Sec. II-A) in a way that the researcher performing the screening could conclude that the focus of the article is in the area of interest. This also excludes articles mentioning these or close terms in the introductory sentences only, particularly articles which main focus was research on security patterns, only referring to privacy as potential application on a side note or as related field of research.

All articles were initially screened independently by two of the authors and classified as "relevant", "irrelevant", or "unclear" by each of them. In case of disagreement or an "unclear" vote regarding relevance, the third author had the casting vote. This way, 30 articles were considered relevant. Another seven articles for which no consensus could be reached were included for further processing to err on the side of safety.

The snowballing step added another 25 articles ranked being relevant, resulting in a total set of 62 relevant articles. The decision on inclusion or exclusion of the articles retrieved by snowballing was made during discussions and consensus among the authors as the much smaller amount of articles retrieved by snowballing allowed for this more direct and time-consuming approach.

C. Keywording and Classification

The keywording of articles was performed based on their abstracts by one author for each article. In many cases, in which the abstracts were considered too short or not sufficiently insightful, the keywording was extended to also cover the introduction, evaluation and conclusion sections. The overall set of articles was keyworded in three iterations. After each iteration, the classification scheme was revised based on any newly discovered keywords, leading to new categories, splitting or merging of categories, or the removal of categories. In particular after the first, but also after later iterations, minor misinterpretations of keywords and categories were discussed and clarified among the authors.

Based on the insights during this step and the adapted reading depth covering more than the abstract, we decided to remove 13 articles from the set of relevant articles, resulting in a total of 49 articles as basis for the mapping and data analysis. These articles are listed separately in the second part of the article's bibliography.

D. Mapping

Five different facets were developed from the keywords derived from the relevant articles in order to address the research question as stated in Sec. I. These five facets are:

- *Type of study:* What kind of study was performed, i.e which research strategy was applied, e.g. a case study or an experiment?
- *Type of contribution:* What is the main contribution of an article? Does it propose one or more patterns, a pattern language, or is its main purpose the evaluation of the use/occurrences of one or more patterns?
- *Addressed software engineering activity:* Which general software engineering activity does an article address?
- *Privacy strategy:* According to Hoepman [19], there exist different strategies to address privacy issues in software. This facet reflects which strategies are primarily supported by the contribution of an article.
- *Class of patterns:* Is the article concerned with patterns, anti-patterns, dark patterns, or related concepts?

During the mapping phase, we also extracted the patterns that were defined in the articles and constructed a separate map at the level of patterns. We performed a mapping of the singular patterns regarding the facets of *software engineering activity*, *class of patterns*, and *addressed privacy strategy*, following the same protocol as for the primary articles.

TABLE I
CATEGORIES OF THE STUDY TYPE FACET.

Category	Description
Philosophical	The study discusses privacy and patterns in a theoretical or abstract context without proposing, evaluating, or using concrete techniques or methods related to privacy and patterns.
Solution Proposal	The study proposes a novel or significant extension of a technique or method related to privacy and patterns; applicability and benefits are shown by a small example or good line of argumentation.
Design & Creation + Case Study	The focus of the study is the development or significant extension of a tool, model or method related to privacy and patterns. Evaluation is performed through a case study (see below).
Design & Creation + Experiment	The focus of the study is the development or significant extension of a tool, model or method related to privacy and patterns. Evaluation is performed through an experiment (see below).
Case Study	The study focuses on a single or a small number of instances of the phenomenon of interest (privacy and patterns), the boundaries of its context are often blurred/unclear.
Experiment	The study focuses on investigating cause and effect relationships in the context of privacy and patterns, carefully excluding undesired factors.
Survey	The study focuses on obtaining the same kind of data from a large group of people/events/systems related to privacy and patterns in a systematic way.

TABLE II
CATEGORIES OF THE CONTRIBUTION TYPE FACET.

Category	Description
Pattern Proposal	The contribution consists of, or deals with, one or more privacy-related patterns (beyond only mentioning a pattern name or reference).
Pattern Catalog	The contribution consists of, or deals with, a set of patterns systematically sorted into different categories.
Pattern Language	The contribution consists of, or deals with, a set of patterns and their interrelationships and interactions.
Pattern Taxonomy	The contribution consists of, or deals with, a categorization of patterns but does not propose concrete patterns.
Modeling Notation	The contribution consists of, or deals with, a notation for modeling privacy-related aspects as patterns or related to patterns, such as threat models.
Analysis Framework	The contribution consists of, or deals with, a conceptual or technical framework for analysing software systems using privacy-related patterns.

E. Replication Package

The artefacts this study bases upon are publicly available in a replication package. This package can be accessed at https://github.com/lenhard/privacy-patterns-replication. It includes the database search queries, the answer sets of these queries, and the maps of categorized papers and patterns.

III. RESULTS

The first facet we look at in this section is the *study type* facet (see Tab. I). The categories are based on two different sources. First, some categories are in line with the empirical research strategies described by Oates, such as *design & creation* research (plus different empirical studies for evaluation), *case studies*, *surveys*, and *experiments* [20]. Further categories are following the suggestions by Wieringa et al., as long as they had not already been covered [21].

The categories of the *software engineering activity* facet correspond to basic activities in software engineering [22]. We identified contributions for the four activities of *requirements engineering*, *architecture*, *design and implementation*, and *quality assurance*. Some articles have been assigned to multiple categories if appropriate. For instance, there are articles that propose patterns for privacy requirements and describe how to transfer them into system design [29].

Fig. 1 illustrates the distributions in terms of numbers of articles classified by the *software engineering activity* and *contribution type* facets aligned with the *study type* facet. Numbers show that most studies are limited to solution proposals, i.e., they propose a new contribution or a significant extension to an existing one, but do not provide empirical evidence to support their contribution. Except for the quality assurance activity, studies are distributed rather evenly on the various activities in software engineering, with the highest number of articles assigned to the architecture category.

Tab. II explains the categories of the *contribution type* facet. As displayed in Fig. 1, the main contributions are pattern proposals. Many pattern proposals are limited to a description of one or two patterns, e.g. [30], [31], [32]. More comprehensive pattern catalogs [33], [34], [35] or languages [36], [37], [38] are rare in absolute numbers.

We also categorised the patterns (148 in total) extracted from the primary studies into regular *patterns*, *antipatterns*, and *dark patterns* according to Bösch et al. [33]. Regular patterns correspond to reusable solutions to common, re-occurring problems, as in the traditional meaning of the term. In contrast, antipatterns are patterns that were initially designed to solve a problem, but turned out to have an adverse effect in practice, in our case effectively compromising or at least not supporting privacy. An example of this is *security images for site verification* [39]. Dark patterns [33], in the context of privacy patterns, have the opposite goal of providing reusable solutions to re-occurring problems in *compromising* privacy. Additionally, the patterns were also categorized according to the software engineering activity they support. Fig. 2 illustrates the numbers in these facets and shows that most of the proposed patterns are regular patterns spread over all the activities. Almost all patterns classified as dark patterns in requirements engineering correspond to threat models that describe how privacy can be compromised, as for example used by Deng et al. [40].

Fig. 2 also illustrates a classification according to strategies as guidelines for privacy engineering and PbD defined by

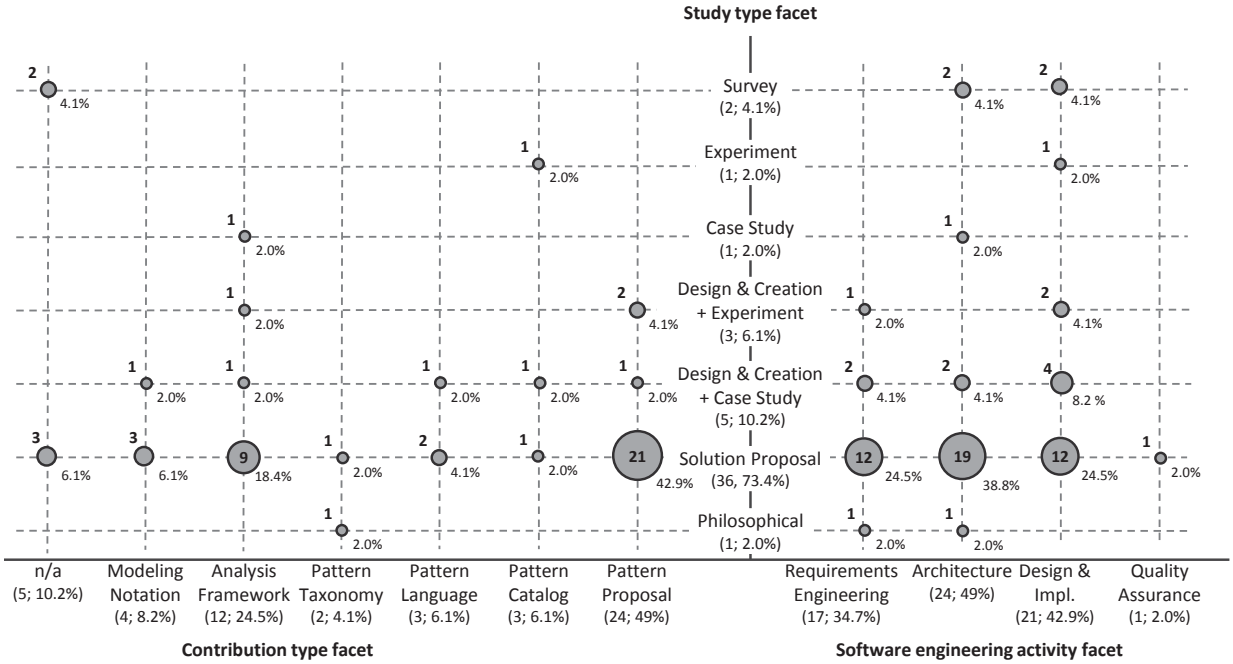

Fig. 1. Numbers of primary studies classified by the study type facet aligned with the contribution type and the software engineering activity facets, respectively. Numbers indicate absolute/relative numbers of papers per category or combination of categories. An article may belong to multiple categories in any facet.

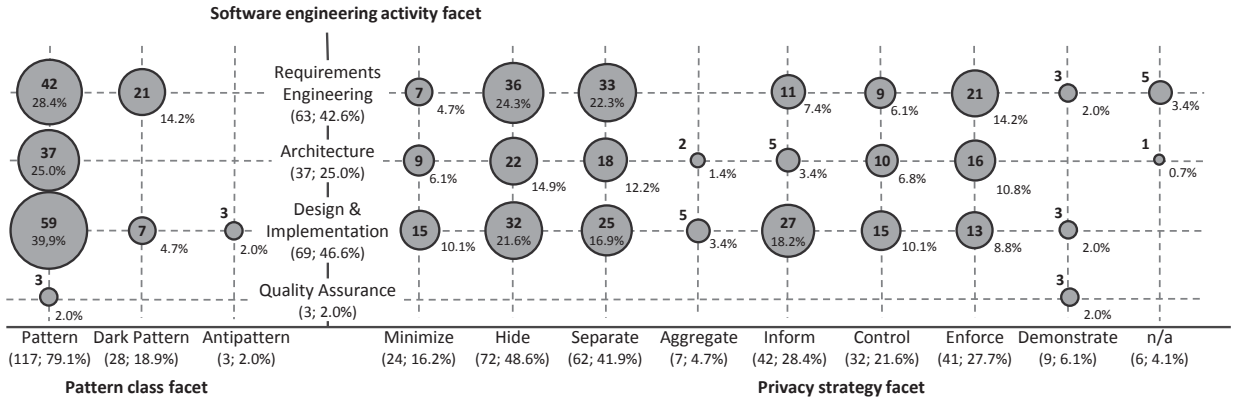

Fig. 2. Numbers of patterns extracted from the primary studies and classified by the software engineering activity facet aligned with the pattern class and the privacy strategy facets. Numbers correspond to absolute/relative numbers of articles per category/combination of category. A pattern may belong to multiple categories in any facet.

Hoepman [19]. These strategies describe fundamental concepts of how privacy concerns can be addressed in IT systems. Two categories of strategies are distinguished: *process-oriented* strategies focus on privacy policies and their communication whereas *data-oriented* strategies focus on properties of data to ensure privacy. Tab. III lists and describes these strategies which we applied to categorize papers into the privacy strategy facet.

The 148 patterns found are distributed unevenly over the different strategies with the *hide* and *separate* standing out. Only few patterns were identified for the strategies *demonstrate* (9) and *aggregate* (7).

IV. Data Synthesis

In this following sections, we discuss the results of the study. We address potential implications and recommend further research actions. Moreover, we outline threats to validity and reliability and countermeasures taken.

A. Interpretation of Results

The results show that there seems to be generally little empirical evidence regarding the relevance, the occurrence, the applicability, or the usage of privacy-related patterns in practice. Of the 49 primary studies that we have found, only twelve studies provide substantial empirical evidence, in form of an experiment, a case study, a survey or design & creation study.

TABLE III
CATEGORIES OF THE PRIVACY DESIGN STRATEGY FACET FOLLOWING THE STRATEGIES PROPOSED AND DESCRIBED BY HOEPMAN [19].

Category	Description
Process oriented	
Enforce	A privacy policy should be in place and be enforced. It should be compatible with legal requirements and constraints.
Demonstrate	The data collecting party should be able to demonstrate that their data processing complies with the privacy policy in place and any applicable legal requirements.
Control	Subjects whose personal data is processed should always be able to control what kind of data about them is processed.
Inform	Subjects whose personal data is processed should be adequately informed whenever their data is processed, by which means and for what purpose.
Data oriented	
Minimize	The amount of personal data processed should be limited to the minimal amount possible, minimizing the potential privacy impact of a system.
Aggregate	Personal data should be processed at the highest level of aggregation at which it is still useful, restricting the level of detail of personal data as far as practically possible.
Separate	Storage or processing of personal data should be performed in separate compartments whenever possible, such that the data cannot easily be used to create complete personal profiles.
Hide	Personal data and their interrelationships should be hidden from plain view.

Case studies are the prevalent research strategy among these studies, either as main strategy or as evaluation strategy in a design&creation approach. Given the prevalence of this research strategy with its potential limitations to the generalizability of results [20] and the overall dominance of non-empirical studies in the field, we must assume that the external validity of the research results on privacy-related patterns as a whole is quite limited. The identified surveys, which in general provide a higher degree of external validity, are mostly contributing to a specialized subfield of interest or are only partially referring to patterns. One of the surveys focuses on the usage of interaction patterns for building user interfaces for privacy notices [41], the other one concentrates on regulatory frameworks and touches upon patterns only briefly [42].

Moreover, the description of the case studies or the experiments in the articles is in most cases very shallow. For example, some articles, which state that they have performed a case study for validating a proposed method, limit the description of the study protocol to a short paragraph mentioning subject groups [29], [43], [44]. Apart from stating that the application of the proposed method was successfully evaluated, further results are hardly reported. It is difficult to evaluate the validity of such case studies or to replicate them based on this level of reporting.

Even though it is an explicitly stated goal of PbD to provide an holistic approach to actually implement privacy-related requirements into IT systems, the research regarding privacy patterns seems quite fragmented in different dimensions. Firstly, there is only little research on how to connect different activities in the development process through patterns related to engineering privacy aspects into software. This is also reflected by the fact that one category of the software engineering activity facet which we originally had had in mind—patterns for the software engineering process as such—did not make it into the final scheme because no paper had been assigned to that category.

Secondly, only very few studies investigate exhaustive pattern catalogues and pattern languages giving advice on how to connect patterns across activities at different stages of the development process and on how patterns related to privacy interrelate with general patterns, such as design patterns, or patterns of other areas, such as security. The pattern catalogues found are quite specialized, such as a dark pattern list [33], cloud privacy patterns [34], and a pattern catalogue tool with a few examples [35]. Pattern languages found relate to privacy user interactions [36], anonymity technology [37], and patterns for collaborative filtering applications in social media [38].

The published research results show a clear focus on the privacy design strategies of *hide* and *separate*. The patterns supporting these two strategies primarily describe encryption and access control schemes, which are classical areas of cryptography and security. On the other hand, a surprising shortage of patterns fitting into the *aggregate* category was found. As anonymization and data transformation, which are typical implementations of this strategy, are widely discussed in the context of big data and information privacy [23], the lack of patterns for these functions is surprising. The low representation of *demonstrate* patterns—which are supposed to demonstrate correct handling of personal data to, e.g. auditors—is another puzzling observation that calls for further investigation facing the transparency requirements of the upcoming GDPR.

B. Implications for Practice and Recommendations for Future Research

It seems that, at the moment, academia provides only little proven or practically validated guidance for practitioners on how to address privacy concerns in engineering software through the use of patterns. We assume though that such guidance would be very helpful as the new GDPR of the EU will be tougher to comply with, especially for software providers less experienced with privacy-regulated domains such as e-healthcare. As this means that little is known about experiences from applying privacy patterns in practice and about practical prerequisites, conditions, etc. applying to them, practitioners might refrain from using them.

Moreover, the available privacy patterns are often quite hard to access not only for practitioners as they often lack required detail and clarity in their descriptions. Comparing patterns and evaluating their usefulness is difficult because descriptions in existing pattern proposals vary strongly in their precision and their level of abstraction.

Furthermore, proposals of isolated patterns are dominating and pattern languages, relating patterns to each other and providing a cohesive single reference for practitioners only

exist for specialized aspects. This, and the lack of approaches addressing the overall software engineering process holistically, might further hinder adoption of privacy patterns in practice at the moment.

In order to increase the field's maturity further and to provide a valuable and verified toolbox for software engineers in practice, we recommend:

1) To harmonize existing privacy pattern-related approaches and privacy patterns, to unify the description format for privacy patterns, and to develop taxonomies to structure the set of privacy patterns available;
2) To develop privacy pattern catalogues and languages that relate patterns for different software engineering activities as well as patterns for other but related aspects such as security patterns or general software design patterns;
3) To further intensify research efforts related to patterns supporting under-represented privacy design strategies, such as *demonstrate* and *aggregate*;
4) To empirically evaluate all aspects of privacy-related patterns and pattern-based approaches, such as their occurrence, usefulness, or applicability in software engineering practice;
5) To broaden the scope of empirical evaluations beyond single case studies, e.g. to conduct surveys and experiments.

Consolidating the area of privacy patterns and improving empirical evidence related to it could significantly help realizing the PbD paradigm and increasing its acceptance in industrial software engineering practice.

C. Validity & Reliability

In this section, we discuss potential validity and reliability issues and describe the actions taken to address them.

We distinguish three types of validity according to the scheme described by Brewer and Crano [24]. *Construct validity* refers to the degree to which measurements taken relate to the studied phenomenon. The studied phenomenon in this work are published research articles related to patterns in privacy, their focus, and the empirical evidence provided. The measurement taken is the sorting of articles into the systematic map based on keyworded abstracts (see Sec. II and Sec. III). We noticed that abstracts sometimes lacked information regarding the categorization scheme or used terms incorrectly, potentially misleading the mapping of such articles. This observation is line with findings from other studies, for example, by Mendes [25]. Being aware of this threat to construct validity, we adapted the reading depth to further sections in cases where the abstract did not provide sufficient information, following the recommendation by Petersen et al. [17].

External validity refers to the degree to which the results of a study can be generalized to a wider population. For this study, this refers to whether the focuses and gaps identified in the reviewed articles are representative for the overall body of published research results. The main threats to external validity in this case are that irrelevant papers might have been included or relevant papers might have been ignored. We tried to mitigate against the risk of missing relevant papers by retrieving articles from four different databases and thoroughly defining the search query strings. Furthermore, we applied snowballing techniques to identify relevant articles not listed in those databases to be as exhaustive as possible and to further minimize the risk.

The third type of validity, *internal validity*, refers to the degree to which a study ensures that a factor, and only this factor, is causing a certain effect. Since this study does not attempt to establish such a causal relationship, we do not consider threats to internal validity here.

Reliability refers to the data gathering and analysis procedures being consistent in the sense that performing gathering and analysis twice will return the same results. A major threat to reliability in literature studies are personal or biased judgements by the participating researchers. To mitigate against this risk, all articles were independently screened by at least two of the authors. In the first step of this screening, involving exactly two authors, 405 out of 480 articles (84,4%) were identically judged. The number increased to 473 articles (98.5%) after involving the third author (see Sec. II-B). The inclusion of papers identified through snowballing was discussed in the group of authors to avoid potential individual bias in that step. The keywording of articles and development of the categorization scheme was performed in iteration, discussing the scheme and refining it after each iteration, to avoid misunderstandings of the categories and to further improve reliability.

V. Related Work

To the best of our knowledge, this mapping study is the first attempt for a literature study in the field of privacy patterns. Nevertheless, several other literature studies from connected fields or with different privacy focus exist.

The most related study from the field of privacy is a mapping study on patient data privacy from 2011 [26]. It assessed what sort of privacy solutions were available in different software development stages, and how they address the U.S. based Markle Foundation's privacy principles for electronic health systems. The study sampled 4670 articles, from which 58 were selected. In the classification of research type, 49 of 58 articles were classified as solution proposals, 6 as a validation study, and 3 as an evaluation. These figures mirrors the prevalence of non-empirical studies that we identified for privacy patterns in a different subfield of privacy engineering.

A recent mapping study on security patterns [27] tried to characterize the current status of the research field based on a map of 30 articles and concluded that research is focused on the application of security patterns. The authors found that slightly more than half of the articles provide a form of experimental evaluation of proposed security patterns which is a considerably higher amount of attempted evaluation than what we have found for privacy patterns which were not mentioned in said study. The higher figures of empirical studies may be due to the maturity of the field of security patterns as an earlier review of security patterns from 2007 attested an overall poor quality in pattern documentation [28]. Although not concerned with privacy patterns specifically, these studies show that empirical

studies in the very closely related field of security patterns become more common, which backs our recommendations regarding these types of studies.

VI. Conclusion

Privacy patterns can be a powerful building block of privacy-by-design which, in turn, might be helpful for software engineers to develop software systems that comply with data protection and privacy regulations such as the GDPR of the EU. The goal of this study was to shed some light on the current state of the research field of privacy patterns.

In this study, we constructed a systematic mapping of the peer-reviewed scientific literature published in that field. We queried four major databases for articles and screened them for relevance, resulting in 49 primary studies on the subject that were subsequently categorized into multiple dimensions. Additionally, we extracted the patterns proposed in the relevant articles, resulting in a set of 148 patterns that were categorized into multiple dimensions as well.

The results show that harmonizing and consolidating the proposed patterns and approaches of the field appear to be important areas for future work. Particularly collecting patterns in pattern languages relating privacy patterns with each other, but also with patterns of general software development and security engineering, might be a task worth pursuing.

Furthermore, there seems to be a large potential for empirical work in this area, such as experiments, case studies, or surveys, and other types of studies that try to substantiate proposed patterns and approaches and provide empirical evidence for (or against) their relevance or benefit. More studies of these types are highly recommended to increase the validity of research in this field.

References

[1] Council of the European Union, "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. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[2] P. Blume, "Impact of the EU General Data Protection Regulation on the public sector," *Journal of Data Protection & Privacy*, vol. 1, no. 1, pp. 53–63, 2016.

[3] S. S. Shapiro, "Privacy by design: Moving from art to practice," *Commun. ACM*, vol. 53, no. 6, pp. 27–29, 2010.

[4] A. Cavoukian, "Privacy by design," *IEEE Technol. Soc. Mag.*, vol. 31, no. 4, pp. 18–19, 2012.

[5] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner, "Privacy and data protection by design-from policy to engineering," European Union Agency for Network and Information Security (ENISA), Tech. Rep., 2014. [Online]. Available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[6] E. Gamma, J. Vlissides, R. Helm, and R. Johnson, *Design patterns: Elements of reusable object-oriented software*. Addison-Wesley, 1995.

[7] F. Buschmann, K. Henney, and D. C. Schmidt, *Pattern-oriented software architecture: on patterns and pattern languages*, 5th ed. Wiley, 2007.

[8] L. Hagge and K. Lappe, "Sharing requirements engineering experience using patterns," *IEEE Software.*, vol. 22, no. 1, pp. 24–31, 2005.

[9] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating security and systems engineering*. Wiley, Dec. 2005.

[10] A. K. Alvi and M. Zulkernine, "A natural classification scheme for software security patterns," in *IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)*, 2011.

[11] G. Lacoste, B. Pfitzmann, M. Steiner, and M. Waidner, *SEMPER - Secure Electronic Marketplace for Europe*, ser. Lecture Notes in Computer Science 1854. Springer, 2000, vol. 1854.

[12] J. Camenisch, D. Sommer, and R. Leenes, *Digital privacy - PRIME - Privacy and Identity Management for Europe*, ser. Lecture Notes in Computer Science. Springer, 2011, vol. 6545.

[13] J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, *Privacy and identity management for life*. Springer, 2011.

[14] H. Roßnagel, J. Camenisch, L. Fritsch, D. Houdeau, D. Hühnlein, A. Lehmann, P. Rodriguez, and J. Shamah, "Futureid-shaping the future of electronic identity," *Datenschutz und Datensicherheit*, vol. 36, no. 3, pp. 189–194, 2012.

[15] N. Doty, M. Gupta, and J. Zych, "privacypatterns.org, web page https://privacypatterns.org/ ,," 2006, accessed on Jan 16, 2017. [Online]. Available: https://privacypatterns.org/

[16] F. Kargl, "privacypatterns.eu," 2016, accessed on Jan 16, 2017. [Online]. Available: https://privacypatterns.eu/

[17] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *12th International Conference on Evaluation and Assessment in Software Engineering*, 2008, Conference Proceedings.

[18] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *18th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, 2014.

[19] J.-H. Hoepman, "Privacy design strategies," in *29th International Conference ICT Systems Security and Privacy Protection (IFIP SEC)*, 2014.

[20] B. J. Oates, *Researching information systems and computing*. London ; Thousand Oaks, Calif.: SAGE Publications, 2006.

[21] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: a proposal and a discussion," *Requir. Eng.*, vol. 11, no. 1, pp. 102–107, 2005.

[22] I. Sommerville, *Software Engineering*, 9th ed. Addison-Wesley, 2011.

[23] J. Domingo-Ferrer, D. Snchez, and J. Soria-Comas, *Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections*. Morgan and Claypool Publishers, 2016.

[24] M. B. Brewer and W. D. Crano, "Research design and issues of validity," *Handbook of Research Methods in Social and Personality Psychology, Second Edition*, pp. 11–26, 2014.

[25] E. Mendes, "A systematic review of web engineering research," in *2005 International Symposium on Empirical Software Engineering, 2005.*, 2005.

[26] I. Masood and S. Zafar, "A systematic mapping study on patient data privacy and security for software system development," in *Sixth Intern. Conf. on Software Engineering Advances (ICSEA)*, 2011.

[27] Y. Ito, H. Washizaki, M. Yoshizawa, T. Okubo, H. Kaiya, A. Hazeyama, N. Yoshioka, and E. B. Fernandez, "Systematic mapping of security patterns research," in *22nd Conference on Pattern Languages of Programs Conference (PLoP)*, 2015.

[28] T. Heyman, K. Yskout, R. Scandariato, and W. Joosen, "An analysis of the security patterns landscape," in *3rd International Workshop on Software Engineering for Secure Systems (SESS)*, 2007.

Appendix

Mapped Primary Studies

[29] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the PriS method," *Requirements Engineering*, vol. 13, no. 3, pp. 241–255, 2008.

[30] N. Ali, D. Jutla, and P. Bodorik, "PIP: An injection pattern for inserting privacy patterns and services in software," in *Privacy Technologies and Policy: 3rd Annual Privacy Forum (APF)*, 2015, pp. 144–157.

[31] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data protection-aware design for cloud services," in *1st International Conference on Cloud Computing (CloudCom)*, 2009.

[32] C. Hillen, "The pseudonym broker privacy pattern in medical data collection," in *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2015.

[33] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side: Privacy dark strategies and privacy dark patterns," *Proceedings on Privacy Enhancing Technologies*, vol. 4, pp. 237–254, 2016.

[34] E. S. Chung, J. I. Hong, J. Lin, M. K. Prabaker, and J. A. Landay, "Development and evaluation of emerging design patterns for ubiquitous computing," in *5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS)*, 2004.

[35] O. Drozd, "Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process," in *10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management. Time for a Revolution?*, 2015.

[36] C. Graf, P. Wolkerstorfer, A. Geven, and M. Tscheligi, "A pattern collection for privacy enhancing technology," in *2nd International Conference on Pervasive Patterns and Applications (PATTERNS)*, 2010.

[37] M. Hafiz, "A pattern language for developing privacy enhancing technologies," *Software: Practice and Experience*, vol. 43, no. 7, pp. 769–787, 2013.

[38] T. Schümmer, "The public privacy-patterns for filtering personal information in collaborative systems," in *Conference on Human Factors in Computing Systems (CHI)*, 2004.

[39] N. Doty and M. Gupta, "Privacy design patterns and anti-patterns," in *A Turn for the Worse: Trustbusters for User Interfaces Workshop*, 2013.

[40] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, 2011.

[41] E. S. Lara, S. R. Murillo, and J. A. Sánchez, "Enhancing privacy notice applications through interaction design," in *4th International Conference in Software Engineering Research and Innovation (CONISOFT)*, 2016.

[42] D. Yimam and E. B. Fernandez, "A survey of compliance issues in cloud computing," *Journal of Internet Services and Applications*, vol. 7, no. 1, pp. 1–12, 2016.

[43] C. Kalloniatis, P. Belsis, E. Kavakli, and S. Gritzalis, "Applying soft computing technologies for implementing privacy-aware systems," in *1st International Workshop on Information Systems Security Engineering (WISSE)*, 2012.

[44] N. Argyropoulos, C. Kalloniatis, H. Mouratidis, and A. Fish, "Incorporating privacy patterns into semi-automatic business process derivation," in *2016 IEEE Tenth International Conference on Research Challenges in Information Science*, 2016.

[45] M. Aljohani, K. Hawkey, and J. Blustein, "Proposed privacy patterns for privacy preserving healthcare systems in accord with nova scotia's personal health information act," in *4th International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*, 2016.

[46] K. Beckers, I. Côté, S. Faßbender, M. Heisel, and S. Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system," *Requirements Engineering*, vol. 18, no. 4, pp. 343–395, 2013.

[47] K. Beckers, S. Faßbender, and H. Schmidt, "An integrated method for pattern-based elicitation of legal requirements applied to a cloud computing example," in *7th International Conference on Availability, Reliability and Security (ARES)*, 2012.

[48] K. Beckers and M. Heisel, "A foundation for requirements analysis of privacy preserving software," in *International Cross-Domain Conference and Workshop on Availability, Reliability, and Security (CD-ARES)*, 2012, pp. 93–107.

[49] C. Bier and E. Krempel, "Common privacy patterns in video surveillance and smart energy," in *7th International Conference on Computing and Convergence Technology*, 2012.

[50] M. Colesky, J. H. Hoepman, and C. Hillen, "A critical analysis of privacy design strategies," in *International Workshop on Privacy Engineering (IPWE)*, 2016.

[51] L. Compagna, P. El Khoury, A. Krausová, F. Massacci, and N. Zannone, "How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns," *Artificial Intelligence and Law*, vol. 17, no. 1, pp. 1–30, 2009.

[52] L. Compagna, P. E. Khoury, F. Massacci, R. Thomas, and N. Zannone, "How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach," in *11th international conference on Artificial Intelligence and Law (ICAIL)*, 2007.

[53] L. F. Cranor, S. Romanowsky, J. Hong, A. Acquisti, and B. Friedman, "Privacy patterns for online interactions," in *Pattern Languages of Programs*, 2006.

[54] A. Cuevas, P. El Khoury, L. Gomez, A. Laube, and A. Sorniotti, "A security pattern for untraceable secret handshakes," in *3rd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, 2009.

[55] E. B. Fernandez, N. Yoshioka, and H. Washizaki, "Patterns for security and privacy in cloud ecosystems," in *2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*, 2015.

[56] M. Hafiz, "A collection of privacy design patterns," in *Pattern languages of programs*, 2006.

[57] D. Hatebur, M. Heisel, and H. Schmidt, "A security engineering process based on patterns," in *18th International Workshop on Database and Expert Systems Applications (DEXA 2007)*, 2007.

[58] J.-H. Hoepman, "Privacy design strategies," in *29th International Conference ICT Systems Security and Privacy Protection (IFIP SEC)*, 2014.

[59] J. Kahrmann and I. Schiering, "Patterns in privacy - a pattern-based approach for assessments," in *9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation*, 2015.

[60] C. Kalloniatis, "Designing privacy-aware systems in the cloud," in *12th International Conference on Trust, Privacy and Security in Digital Business*, 2015.

[61] A. Kung, "Pears: Privacy enhancing architectures," in *Privacy Technologies and Policy: 3rd Annual Privacy Forum (APF)*, B. Preneel and D. Ikonomou, Eds. Springer, 2014.

[62] T. Länger, H. C. Pöhls, and S. Ghernaouti, "Selected cloud security patterns to improve end user security and privacy in public clouds," in *Privacy Technologies and Policy: 4th Annual Privacy Forum (APF)*, 2016.

[63] L. L. Lobato, E. B. Fernandez, and S. D. Zorzo, "Patterns to support the development of privacy policies," in *4th International Conference on Availability, Reliability and Security (ARES)*, 2009.

[64] M. S. Mahmud and S. L. Osborn, "Tradeoff analysis of relational database storage of privacy preferences," in *9th Secure Data Management VLDB Workshop (SDM)*, 2012.

[65] P. Mehregan and P. W. L. Fong, "Design patterns for multiple stakeholders in social computing," in *28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec)*, 2014.

[66] R. Meis, "Problem-based consideration of privacy-relevant domain knowledge," in *8th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6 International Summer School on Privacy and Identity Management for Emerging Services and Technologies*, 2013.

[67] S. Pearson and A. Benameur, "A decision support system for design for privacy," in *6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School on Privacy and Identity Management for Life*, 2010.

[68] S. Pearson and Y. Shen, "Context-aware privacy design pattern selection," in *7th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, 2010.

[69] J. Porekar, A. Jerman-Blazic, and T. Klobucar, "Towards organizational privacy patterns," in *2nd International Conference on the Digital Society*, 2008.

[70] A. C. Porisini, P. Colombio, and S. Sicari, "Dealing with anonymity: Design patterns for privacy-aware systems," in *International Conference on Software Technology and Engineering (ICSTE)*, 2009.

[71] J. v. Rest, D. Boonstra, M. Everts, M. v. Rijn, and R. v. Paassen, "Designing privacy-by-design," in *Privacy Technologies and Policy: 1st Annual Privacy Forum (APF)*, 2012.

[72] M. Sadicoff, M. M. Larrondo-Petrie, and E. B. Fernandez, "Privacy-aware network client pattern," in *12th Pattern Languages of Programs Conference (PLoP)*, 2005.

[73] M. Schumacher, "Security patterns and security standards - with selected security patterns for anonymity and privacy," in *European Conference on Pattern Languages of Programs (EuroPLoP)*, 2002.

[74] J. Siljee, "Privacy transparency patterns," in *20th European Conference on Pattern Languages of Programs (EuroPLop)*, 2015.

[75] S. Strauch, U. Breitenbuecher, O. Kopp, F. Leymann, and T. Unger, "Cloud data patterns for confidentiality," in *2nd International Conference on Cloud Computing and Service Science (CLOSER)*, 2012.

[76] X. Xuan, Y. Wang, and S. Li, "Privacy requirements patterns for mobile operating systems," in *4th International Workshop on Requirements Patterns (RePa)*, 2014.

[77] J. D. Young, "Commitment analysis to operationalize software requirements from privacy policies," *Requir. Eng.*, vol. 16, no. 1, pp. 33–46, 2010.