A Taxonomy of Requirements for the Privacy Goal Transparency (Technical Report)

Rene Meis, Roman Wirtz, and Maritta Heisel

paluno - The Ruhr Institute for Software Technology – University of Duisburg-Essen
{firstname.lastname}@paluno.uni-due.de

Foreword

This technical report presents the details of the literature review performed for the research paper [1].

Abstract. Privacy is a growing concern during software development. Transparency–in the sense of increasing user's privacy-awareness–is a privacy goal that is not as deeply studied in the literature as the properties anonymity and unlinkability. To be compliant with legislation and standards, requirements engineers have to identify the requirements on transparency that are relevant for the software to be developed. To assist the identification process, we provide a taxonomy of transparency requirements derived from legislation and standards. This taxonomy is validated using related research which was identified using a systematic literature review. Our proposed taxonomy can be used by requirements engineers as basis to systematically identify the relevant transparency requirements leading to a more complete and coherent set of requirements.

1 Introduction

The awareness for privacy concerns is growing in the public. With this awareness comes a call for more transparency on what, why and how software-systems collect, use, and process personal information. Hansen [2] identifies transparency as one of three privacy protection goals ensuring *"that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed"* [3]. Hence, it is not sufficient to increase user's privacy awareness, it is also necessary to provide the information needed to users in order to understand how they personal data is processed. Transparency, as all software qualities, is a complex property. It leads to requirements for the representation of static information about the software's intended purpose, but also to requirements on informing users about run-time events, e.g., malfunctions. In addition to the requirements about informing *what* happens, there are also requirements on *how* the information is shown to users to ensure that mechanisms to improve the software's transparency have an impact on the user's privacy-awareness. Especially concerning legal compliance, requirements engineers have to provide an as complete set of requirements as possible to ensure that the software that is built based on these requirements is compliant. I.e., the software requirements have to bridge the gap between the legal requirements and the technical mechanisms to realize them. To empower requirements engineers to identify all transparency requirements relevant for the software to be built, we have to refine the high-level privacy goal transparency into more concrete transparency requirements that assist requirements engineers in the elicitation process.

To obtain an as complete taxonomy of transparency requirements as possible, we consider different sources that requirements engineers also should consider. To be compliant with legislation requirements engineers have to consider privacy and data protection laws relevant to them, depending on the application domain of the software to be developed also standards have to be considered, to increase user acceptance, the user's needs have to be considered. We used as sources for the creation of our taxonomy the ISO/IEC 29100:2011 standard [4] and the draft of the EU Data Protection Regulation [5]. We then considered relevant research in the field of privacy, transparency, and awareness including empirical research on user's privacy concerns to validate the completeness of the proposed taxonomy.

The rest of the paper is structured as follows. Our privacy requirements taxonomy is derived and presented in Section 2 and validated using related work identified using a systematic literature review in Section 3. Section 4 concludes the paper.

2 Deriving and Structuring Requirements on Transparency

In Section 2.1, we systematically analyze the privacy principles described by ISO/IEC 29100:2011 [4] and the draft of the EU data protection regulation [5] to derive the transparency requirements they contain. To derive the requirements, we analyzed the description of the privacy principles and the formulations of the regulation. We looked for verbs like *inform*, *notify*, *document*, *present*, *provide*, *explain*, *communicate* and related nouns. We keep the formulation of the identified transparency requirements close to the original documents from which we identified them. In Section 2.1, we enumerate these derived requirements using the notation Tn. As the ISO principles and EU articles partly overlap, we identified several refinements of identified requirements. We relate those requirements using a *refines* relation. If a transparency requirements Tn_1 refines a part of another requirement Tn_2, this means that Tn_1 adds further details on how or what information has to be made transparent. The *refines* relation is visualized in form of an initial ontology of transparency requirements in Fig. 1. In Section 2.2, we structure the transparency requirements identified in Section 2.1 into a taxonomy of transparency requirements. This taxonomy is presented as an extensible metamodel.

ISO/IEC 29100:2011 and the draft of the EU data protection regulation do not use the same terminology. To avoid ambiguities, we will use the following term definitions from the draft of the EU data protection regulation in this paper.

Data subject *"means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."* This term is called *PII principal* in ISO/IEC 29100:2011.

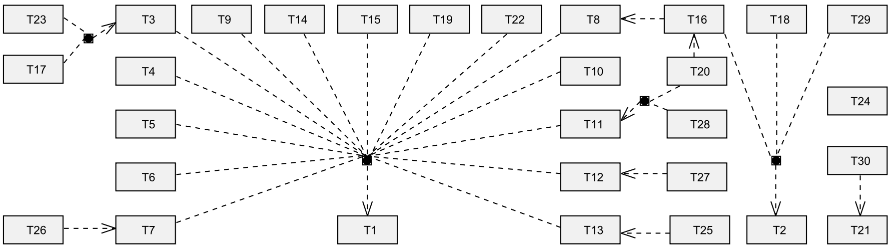

Fig. 1. Initial ontology of transparency requirements

Personal data *"means any information relating to a data subject."* This term is called *personally identifiable information (PII)* in ISO/IEC 29100:2011.

Processing *"means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction."*

Controller *"means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law."* This term is called *PII controller* in ISO/IEC 29100:2011.

2.1 Requirements Identification from Privacy Principles and Legislation

ISO/IEC 29100 Privacy Principles To derive our taxonomy of transparency requirements, we first consider the international standard ISO/IEC 29100:2011 [4], which defines 11 privacy principles which are a superset of the OECD principles [6] and the US fair information practices (FIPs) [7].

We start our analysis of the privacy principles with the *openness, transparency and notice principle*, which is obviously concerned with transparency. From this principle, we obtain the following transparency requirements.

T1 Inform data subjects about the controller's policies, procedures and practices with respect to the processing of personal data.
T2 The information about the management of personal data has to be clear and easily accessible for data subjects (and the public).
T3 Explain the purpose of data processing to data subjects.
T4 Specify the persons to whom the personal data might be disclosed.
T5 Provide the identity of the controller including contact information to data subjects.
T6 Provide information about the choices to limit the processing of personal data to data subjects.

T7 Provide information about the means to access, correct and remove personal data to data subjects.
T8 Provide information in the case that a decision that a data subject can make has an impact on the data subject.
T9 Document and communicate all contractual obligations that impact personal data processing externally to the extent those obligations are not confidential.
T10 Provide information about the personal data required for the specified purpose to data subjects.
T11 Provide information about how and what personal data is collected to data subjects.
T12 Provide information about how, what and to whom personal data is communicated to data subjects.
T13 Provide information about how and what personal data is stored to data subjects.
T14 Provide information about authorized natural persons who will access personal data to data subjects.
T15 Provide information about data retention and disposal requirements.

T1 and T2 are the most general requirements in our initial ontology. Hence, they form the root elements (cf. Fig. 1). T1 is considered with *what* information has to be presented and is refined by T3-T15 that are all also concerned with about what data subjects have to be informed. In contrast, T2 is concerned with *how* that information has to be presented to data subjects.

The *consent and choice principle* strengthens that data subjects have to give their consent on a *"knowledgeable basis"* and hence, they have to be informed before obtaining consent. This information has also to contain information about *"the implications of granting or withholding consent"*. We identify the following requirement.

T16 Before data subjects are asked to give consent to use their data, provide all information necessary to make this decision to them, including the implications of granting or withholding consent.

This requirement refines T2 in the sense that the point in time when the information has to be provided is specified. Additionally, T16 refines T8 by describing which data has to be provided to data subjects when they make the decision to give consent.

The principle *purpose legitimacy and specification* stresses that data subjects have to be informed about the purpose of data collection and use before it is used for the first time or for a new purpose. This information has to be presented using language *"which is both clear and appropriately adapted to the circumstances*. In the case that sensitive data is processed, sufficient explanations have to be provided to the data subject. Hence, we obtain following requirements.

T17 Inform data subjects about the purpose of data collection and use before it is collected or used for the first time for this purpose.
T18 The language used for providing information to data subjects has to be clear and appropriately adapted to the circumstances.
T19 Provide sufficient explanations whenever sensitive data is used to data subjects.

Requirement T17 complements T3 with the information when data subjects have to be informed. T18 is a refinement of T2 by adding the notice that the presentation has to be adapted to the circumstances in which this information is shown. T19 places emphasis on providing explanations whenever sensitive data is used and hence refines the top-level requirement T1.

The principle *collection limitation* is concerned with limiting the collected personal data to the minimum needed. We obtain the following additional requirement.

T20 Provide information to data subjects about if it is optional to provide personal data.

This requirement complements T11 and T16, because it is important to inform data subjects before data collection and giving consent whether it is optional to provide the questioned personal data .

The principle *accountability* contains the following transparency requirements that are concerned with the occurrence of privacy breaches, which is not yet covered by other transparency requirements, because the other requirements are concerned with the normal behavior of the system under consideration.

T21 Inform data subjects and other relevant stakeholder (as required in some jurisdictions) about privacy breaches that can lead to substantial damage to data subjects as well as the measures taken for resolution.

The principle *information security* implies the following transparency requirement that refines the transparency requirement T1.

T22 Inform data subjects about the (security) mechanisms to protect their personal data.

Draft of the EU Data Protection Regulation To identify further transparency requirements and to refine the already identified requirements, we analyze the draft of the EU Data Protection Regulation [5] that is currently under review and will be when accepted by all member states be mandatory to be implemented by all EU member states. In contrast to the situation in the US where no privacy regulations covering all industrial branches exist [8], the EU Data Protection will cover all industrial branches.

Article 5 (b) adds the need that the purpose has to be legitimate to requirement T3. Hence, we obtain the following refined requirement.

T23 Explain data subjects why the purpose of data collection is legitimate.

Article 12 prescribes the implementation of procedures and mechanisms for exercising the rights of data subjects and says that *"If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy."*. Hence, we identify a transparency requirement that, similar to T21, is not concerned with the normal system behavior.

T24 If requests of data subjects for exercising their rights are rejected, then the reasons for the refusal has to be provided.

From Article 14, we can derive following transparency requirements that refine previously identified requirements.

T25 Provide the period for which the personal data will be stored to data subjects.

T26 Provide information about *“the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data”*

T27 Provide information about data transfer *“to a third country or international organisation and the level of protection afforded by that third country or international organization”*.

T28 Inform the data subject about the source the personal data used originates from.

T29 Provide information to data subjects *“at the time when the personal data are obtained from the data subject; or where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.”*

T25 refines T13 by adding the need for specifying the duration of data storage. T26 adds a legal need to T7. T27 refines T12 by requiring special treatment when data is transferred to third countries or international organizations. T28 refines T11 by adding the need to provide information of the source of the personal data used. T29 refines T2 with information about when to provide information to data subjects.

Article 31 is concerned with the notification of personal data breaches and refines T21 by adding a duration after which the supervisory authorities have to be informed.

T30 Notify supervisory authorities (and data subjects) about the occurrence of a personal data breach not later than 24 hours after having become aware of it.

2.2 Setting up a Transparency Requirements Taxonomy

In this section, we structure the identified preliminary transparency requirements into a transparency requirements taxonomy. Figure 2 shows our taxonomy in the form of a metamodel using a UML class diagram. We structured the transparency requirements into a hierarchy, which is derived from the initial ontology shown in Fig. 1. We describe our taxonomy in the following from the top to the bottom. An overview of the mapping between the transparency requirements taxonomy to the initial transparency requirements is given in Table 1.

Transparency Requirement The top-level element of our hierarchy is the general *TransparencyRequirement* which corresponds to the initial requirement T1. In our metamodel we declared this requirement as *abstract*, i.e., it is not possible to instantiate it, only its specializations can be instantiated. It has six attributes. First, the dataSubject who has to be informed. Second, a set of counterstakeholders who are involved in the processing of the data subject’s data and the data subject has to be informed about them. For example, T4 and T14 prescribe to specify the (authorized) persons to whom personal data might be disclosed. This is the case for many requirements in our taxonomy and hence, we put this attribute to the top-level requirement. If there is no need to specify persons who are somehow involved in the data processing, the attribute counterstakeholder is left empty. Our taxonomy suggests to consider data subjects and counterstakeholders as persons. The data subject should be a natural person, whereas

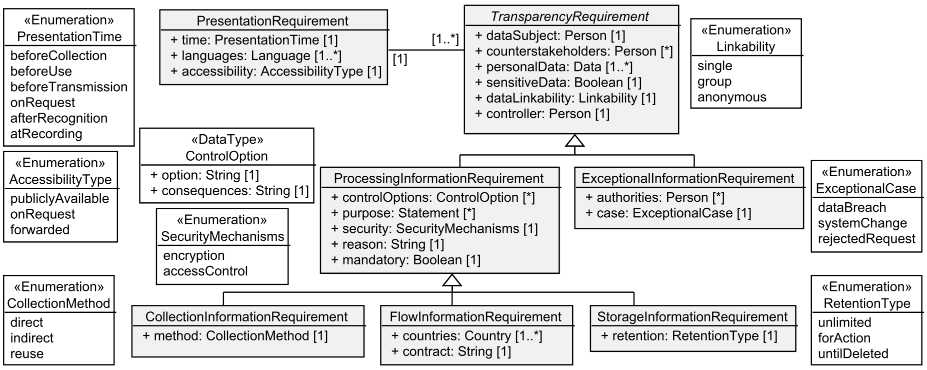
«Enumeration» PresentationTime
beforeCollection
beforeUse
beforeTransmission
onRequest
afterRecognition
atRecording
PresentationRequirement
+ time: PresentationTime [1]
+ languages: Language [1..*]
+ accessibility: AccessibilityType [1]
[1..*]
[1]
TransparencyRequirement
+ dataSubject: Person [1]
+ counterstakeholders: Person [*]
+ personalData: Data [1..*]
+ sensitiveData: Boolean [1]
+ dataLinkability: Linkability [1]
+ controller: Person [1]
«Enumeration» Linkability
single
group
anonymous
«Enumeration» AccessibilityType
publiclyAvailable
onRequest
forwarded
«DataType» ControlOption
+ option: String [1]
+ consequences: String [1]
«Enumeration» SecurityMechanisms
encryption
accessControl
ProcessingInformationRequirement
+ controlOptions: ControlOption [*]
+ purpose: Statement [*]
+ security: SecurityMechanisms [1]
+ reason: String [1]
+ mandatory: Boolean [1]
ExceptionalInformationRequirement
+ authorities: Person [*]
+ case: ExceptionalCase [1]
«Enumeration» ExceptionalCase
dataBreach
systemChange
rejectedRequest
«Enumeration» CollectionMethod
direct
indirect
reuse
CollectionInformationRequirement
+ method: CollectionMethod [1]
FlowInformationRequirement
+ countries: Country [1..*]
+ contract: String [1]
StorageInformationRequirement
+ retention: RetentionType [1]
«Enumeration» RetentionType
unlimited
forAction
untilDeleted

Fig. 2. Our proposed taxonomy of transparency requirements.

Table 1. Mapping of transparency requirements to preliminary requirements

Requirement	Attribute	Tn
TransparencyRequirement	data subject, personal data	T1
	controller	T5
	counterstakeholder	T4, T14
	linkability	T16
	sensitiveData	T19
PresentationRequirement	accessibility	T2
	language	T18
	time	T16, T29, T30
ExceptionalInformationRequirement	case	T17, T21, T24, T30
	authorities	T21
ProcessingInformationRequirement	controlOptions	T6, T7, T8, T26
	mandatory	T10, T20
	purpose, reason	T3, T17, T23
	security	T22
CollectionInformationRequirement	method	T11, T28
StorageInformationRequirement	retention	T13, T15, T25
FlowInformationRequirement	contract, country	T9, T12, T27

the counterstakeholders can be natural, legal, or artificial persons, e.g., organizations or authorities. Third, the set of personal data of the data subject for which the transparency requirement is relevant. Almost all transparency requirements that we identified previously refer to the data subject and his/her personal data. Hence, all transparency requirements in our taxonomy have the data subject and his/her personal data as attribute. Fourth, we document whether the specified personal data represents senstiveData, because of T19 sensitive data needs special consideration. Fifth, the attribute linkability documents whether the personal data is linkable to a single data subject, a group of possible data subjects, or is anonymous. This attribute is not explicitly motivated from the requirements, but T16 mentions that in the case of giving consent all information necessary to make this decision has to be provided to data subject and we think that the linkability of the personal data to the data subject is such an information. Sixth, in accordance with T5 the data subject has to be informed about who the controller is.

Presentation Requirement The initial transparency requirements T2, T16, T18, T29, and T30 are in contrast to the other requirements not mainly concerned with *what* information shall be provided to the data subject, but with *how* this information has to be presented. To decouple the *how* from the *what* in our taxonomy, we introduce PresentationRequirements. Every TransparencyRequirement has exactly one PresentationRequirement assigned, which describes how the information has to be provided to the data subject. On the other side, the same PresentationRequirement can be related to multiple TransparencyRequirements. The attribute time reflects T16, T29, and T30 that prescribe the time when information has to be provided. The possible values for this attribute are summarized in the enumeration PresentationTime (cf. Fig. 2). We derived these values from T16, T29 and T30. Nevertheless, we do not consider this enumeration, such as all other enumerations presented in our taxonomy, as complete and whenever necessary they can be extended. The attribute languages is not explicitly mentioned in a transparency requirement, but to provide information clearly and adapted to the circumstances to data subjects (in accordance with T18) one should present this information using at best the first language of each possible data subject. The attribute accessibility serves to document the requirements on how data subject shall be able to access the information, indicated by T2. An information may has to be publiclyAvailable, onRequest of the data subject, or the information is forwarded to the user when needed.

ExceptionalInformationRequirement Most transparency requirements are concerned with providing information about the normal behavior of the considered system. This information can be considered as rather static. In contrast, T21, T24, and T30 require to inform data subjects in cases where unexpected events occur. For this purpose, we refine the general TransparencyRequirement into the requirement ExceptionalInformationRequirement. The attribute case stores the kind of unintended event the data subject has to be informed about. This can be a dataBreach as mentioned in T21 and T30, a systemChange that e.g., changes the purpose of data processing (cf. T17), or a rejectedRequest of a data subject as described in T24. In addition to the data subject that has to be informed, T21 also states that authorities may have to be informed. The attribute authorities is used to document the natural, legal, or artificial persons that have to be informed if the respective exceptional case occurs.

ProcessingInformationRequirement The requirement ProcessingInformationRequirement refines TransparencyRequirements and contains the properties that all *static* transparency requirements, which refine the initial requirement T1 (cf. Fig. 1), have in common. The attribute controlOptions summarizes (using the data type ControlOption) the options the data subject has to limit the processing of personal data (T6), means to access, correct and remove personal data (T7 and T26), and the consequences implied by these options (T8). T3, T17, and T23 require that the purpose for data processing is explained to data subjects. The attribute purpose is used to provide a set of Statements that could consist of functional requirements and knowledge about the software environment for which's fulfillment the personal data of the data subject is needed. Furthermore, the attribute reason is used to provides information about why the personal data is needed for the purpose and why it is legitimate to use it. Due to T10 and T20, data subjects have to be clearly informed whether the provision of personal data is optional and whether the information is needed for the specified purpose. The attribute mandatory is used to capture this information. The attribute security is used to represent how the personal data is protected as required by T22. Possible protection mechanisms are e.g., encryption and accessControl.

CollectionInformationRequirement Requirement T11 prescribes that data subjects have to be informed about how and what data is collected from them. For this purpose, we refined the ProcessingInformationRequirement into the CollectionInformationRequirement. In addition to the information that is already inherited from TransparencyRequirement and ProcessingInformationRequirement, we derived from T28, which is a refinement of T11 (cf. Fig. 1), the attribute method that reflects whether the data collection is direct, indirect, or whether existing data of the subjects is reused.

FlowInformationRequirement Requirement T12 implies a further refinement of ProcessingInformationRequirement that we call FlowInformationRequirement. This requirement prescribes to inform data subjects about the flow of their data. From T9 and T27, we derived that for each information flow, it is important to inform the data subject about the contractual obligations and policies the data receiver is bound to. This information is represented in the attribute contract. Furthermore, T27 puts an emphasis on taking care of data transfer to *third countries* and international organizations. Hence, we added the attribute countries to capture the geographical destination of the data flow.

StorageInformationRequirement From T13, we derive the requirement StorageInformationRequirement that is also a refinement of ProcessingInformationRequirement. This requirement is used to represent the information that is needed to inform the data subject about the storage of his/her personal data. In addition to the attributes inherited from TransparencyRequirement and ProcessingInformationRequirement, T15 and T25 require that the data subject is informed about the duration of storage and the data retention and disposal requirements. To reflect this information, we use the attribute retention. The possible values of this attribute can indicate that personal data is stored for an unlimited time, as long as it is needed for the purpose it was collected for (forAction), or until it is deleted (untilDeleted) after there is no reason to keep the data anymore, but not directly.

The complete taxonomy is shown in Fig. 2. Note that the taxonomy is easily extensible by further refinements of requirements, adding further attributes and relations, and adapting the suggested enumerations to the needs implied by the application domain and relevant legislation of the software to be developed. Table 1 provides an overview of how the initial requirements Tn that we derived from ISO 29100 and the draft of the EU Data Protection Regulation are reflected by the proposed taxonomy.

3 Validation of the Taxonomy Using Related Literature

In this section, we give an overview of existing research that also contains considerations about the privacy goal of transparency. To validate our proposed taxonomy, we map the notions and concepts used in the related literature to our taxonomy to check whether it is suitable to reflect the shapes of transparency used in the literature.

To identify the relevant related work, we performed a systematic literature review using backward snowballing [47]. To obtain the starting set of papers for our review, we manually searched the proceedings and issues of the last 10 years of computer sci-

Table 2. Overview of Sources for the Literature Review

Name	Abbr.	Type	Rank	Final	First
IEEE Symposium on Security and Privacy	S&P	Conf	A*	1	11
International Conference on Software Engineering	ICSE	Conf	A*	1	4
ACM SIGSOFT Int. Symp. on the Foundations of Software Engineering	FSE	Conf	A	0	3
IEEE International Conference on Trust, Security and Privacy in Computing and Communications	TrustCom	Conf	A	1	45
IEEE International Requirements Engineering Conference	RE	Conf	A	1	23
International Conference on Advanced Information Systems Engineering	CAiSE	Conf	A	0	6
ACM/SIGAPP Symposium On Applied Computing	SAC	Conf	B	1	10
European Software Engineering Conference	ESEC	Conf	B	0	2
IFIP Information Security & Privacy Conference	IFIP-SEC	Conf	B	1	17
International Conference on Availability, Reliability and Security	ARES	Conf	B	1	21
International Conference on Trust, Privacy and Security in Digital Business	TrustBus	Conf	B	3	38
International Joint Conference on Software Technologies	ICSOFT	Conf	B	0	1
International Working Conference on Requirements Engineering: Foundation for Software Quality	REFSQ	Conf	B	0	5
Symposium On Usable Privacy and Security	SOUPS	Conf	B	1	28
ACM Transactions on Computer Systems	TOCS	Jour	A*	0	0
ACM Transactions on Software Engineering and Methodology	TOSEM	Jour	A*	0	1
IEEE Transactions on Software Engineering	TSE	Jour	A*	1	6
Journal of Computer and System Sciences	JCSS	Jour	A*	0	1
Journal of Computer Information Systems	JCIS	Jour	A	1	8
Journal of Systems and Software	JSS	Jour	A	1	7
Software: Practice and Experience	SPE	Jour	A	0	4
Advances in Engineering Software	AES	Jour	B	0	1
Computer Law and Security Report	CL&SR	Jour	B	2	18
Computer Standards and Interfaces	CSI	Jour	B	1	3
IEEE Security and Privacy Magazine	S&P	Jour	B	6	51
IEEE Software	Software	Jour	B	1	4
Information and Software Technology	IST	Jour	B	0	1
International Journal of Software Engineering and Knowledge Engineering	IJSEKE	Jour	B	0	0
Journal of Computer Science and Technology	JCST	Jour	B	0	0
Journal of Computer Security	JCS	Jour	B	0	2
Journal of Software	JSW	Jour	B	0	5
Requirements Engineering	RE	Jour	B	2	9
Software and System Modeling	SOSYM	Jour	B	0	0
Backward Snowballing	-	-	-	13	68

ence conferences and journals that are mainly concerned with at least one of the topics privacy, requirements, and software engineering and ranked at least as *B-level* in the CORE2014[1] ranking. The list of considered conferences and journals is shown in Table 2. First, we checked whether title or abstract of a paper indicated that the paper is concerned with privacy (requirements), transparency, or awareness (row First in Table 3). If this was the case, we analyzed the full text of the paper (row Final in Table 3). Due to the manual search process, we have to deal with the threat of validity that our starting set of papers does not contain all relevant literature, because it was published in a source that we do not consider or was published earlier than in the last 10 years, To mitigate this threat, we applied backward snowballing. I.e., we also considered the papers referenced in the papers that we identified as relevant until no new candidates

[1] `http://www.core.edu.au/coreportal`

Table 3. Detailed mapping of transparency notions from the literature to our proposed taxonomy - Part 1

Privacy (Requirements) Engineering							
Source	**Mentioned Concept**	**PR**	**EIR**	**PIR**	**SIR**	**FIR**	**CIR**
Breaux [9]	Increase awareness	X					
Deng et al. [10]	Content awareness			X	X	X	X
	Policy and consent compliance		X	X	X	X	X
Feigenbaum [11]	Collection Limitation						X
	Purpose Disclosure (Notice)	X		X			
Fhom and Bayarou [12]	Ensuring Customers Empowerment and Transparency			X	X	X	
Hedbom [13]	Provide information			X	X	X	X
Hoepman [14]	Inform		X	X	X	X	
Kung et al. [15]	Transparency			X	X	X	X
Langheinrich [16]	Notice	X					X
Masiello [17]	Intelligible Transparency	X		X	X	X	X
Miyazaki et al. [18]	Provide purpose			X			
	Information breach		X				
Mouratidis et al. [19,20]	Provider's transparency			X			
	Organizational policies	X		X			
Pötzsch [21]	Requirements	X		X		X	
Rost and Pfitzmann [22], Hansen [2], Bier [23]	Transparency			X	X	X	X
Spiekermann and Cranor [24]	Combining Data			X			
	Future attention consumption	X					
	Internal/external unauthorized transfer					X	
	Internal/external unauthorized processing			X			
	Unauthorized collection of data from client and exposure						X
Wicker and Schrader [25]	Provide full disclosure of data collection	X		X	X	X	X
	Require Consent to Data Collection	X		X			

PR: PresentationRequirement, **EIR**: ExceptionalInformationRequirement,**PIR**: ProcessingInformationRequirement, **SIR**: StorgeInformationRequirement, **FIR**: FlowInformationRequirement, **CIR**: CollectionInformationRequirement

were found. In total, we identified 403 papers that seemed to be relevant after reading title and abstract. After the analysis of the full text, we finally identified 39 papers as related work.

In the following, we provide an overview of the identified literature and discuss whether and how our taxonomy reflects the concepts mentioned in the literature. Table 3 and Table 4 summarize the discussion. We categorized the identified literature into the four categories *Privacy (Requirements) Engineering*, *Empirical Research on Privacy Awareness*, *Privacy from the Legal Perspective*, and *Privacy Policies and Obligations*.

3.1 Privacy (Requirements) Engineering

Spiekermann and Cranor [24] provide an overview of the field of privacy engineering and systematically structure the topics in this field of research. The authors provide an overview of best practices for providing privacy notices to data subjects based on concerns data subjects may have. The concern *combining data* needs to inform the data subject about the linkability of his/her personal data. *future attention consumption* needs to inform how the data subject is planned to be contacted when necessary. The concern *internal/external unauthorized transfer* needs to inform about data flows and with whom information is shared. *internal/external unauthorized processing* needs to provide the purpose of data processing to data subjects. The concerns *unauthorized collection of data from client* and *exposure* indicate that the data subject shall be informed about how and what personal information is collected. These concerns can be mapped to the requirements of our taxonomy as shown in Table 3.

The LINDDUN-framework proposed by Deng et al. [10] is an extension of Microsoft's security analysis framework STRIDE [48]. The basis for the privacy analysis is a data flow diagram (DFD) which is then analyzed on the basis of the high-level threats Linkability, Identifiabilitiy, Non-repudiation, Detectability, information Disclosure, content Unawareness, and policy/consent Noncompliance. Hence, LINDDUN considers the high-level transparency goal *content awareness* and the goal *policy and consent compliance*, which are related to transparency requirements. These goals can be mapped to the requirements of our taxonomy as shown in Table 3.

Hoepman [14] proposes eight privacy design strategies to support people involved in the conceptual development and analysis phase of software development to address the privacy principles of the OECD guidelines [6], ISO 29100 [4], and the EU data protection directive [49]. The relevant privacy design strategy for transparency is called *INFORM*. Hoepman describes this strategy as follows: *"Whenever data subjects use a system, they should be informed about which information is processed, for what purpose, and by which means. This includes information about the ways the information is protected, and being transparent about the security of the system. Providing access to clear design documentation is also a good practice. Data subjects should also be informed about third parties with which information is shared. And data subjects should be informed about their data access rights and how to exercise them."* All these aspect were also identified by us and hence, we can map the inform strategy as shown in Table 3.

Rost and Pfitzmann [22], and Hansen [2] introduce the privacy protection goals *unlinkability*, *transparency*, and *intervenability* that complement the standard security protection goals *confidentiality*, *integrity*, and *availability* and discusses the importance of considering all these goals during system design. According to Hansen *"Transparency aims at an adequate level of clarity of the processes in privacy-relevant data processing so that the collection, processing and use of the information can be understood and reconstructed at any time. Further, it is important that all parties involved can comprehend the legal, technical, and organizational conditions setting the scope for this processing. This information has to be available before, during and after the processing takes place."* Hence, we obtain the mapping shown in Table 3. Bier [23] also uses Hansen's definition of transparency.

Fhom and Bayarou [12] describe a methodological framework for a privacy engineering method for smart grid systems. One principle of their framework is *Ensuring Customers Empowerment and Transparency*. This principle aims at providing data subjects information that allows them *"understand how their personal data would be handled"*. Hence, this principle is related to the processing information requirement and its subrequirements as shown in Table 3.

Mouratidis et al. [19,20] propose a framework that supports the selection of cloud providers based on security and privacy requirements. In their framework the authors discuss nine security and privacy issues that have to be addressed. The issue *provider's transparency* suggests to inform data subjects about the security mechanisms used to secure their personal data. The issue *Organisational policies* needs to inform data subjects about the processing of their personal data in an unambiguous and understandable way. These issues can be mapped to the requirements of our taxonomy as shown in Table 3.

Masiello [17] argues that one of the biggest issues with privacy is the question: *"How do we create transparency that's accessible to average users, such that their choices are adequately informed?"* To address this question, all necessary information has to be collected and presented in an appropriate way. Our taxonomy shall help to elicit the relevant information to do so.

Hedbom [13] performed a survey on transparency tools and identifies requirements for these tools. Hedbom states that transparency tools shall *"gives information on intended collection, storage and/or data processing to the data subject, or a proxy acting on the behalf of the data subject, in order to enhance the data subject's privacy"*. This can be addressed by our taxonomy as shown in Table 3.

Breaux [9] elaborates on the current privacy needs and provides recommendations for developers to follow. One of these recommendations is *increase awareness*. This recommendation says that it is important that user notifications are provided in a way that they are recognized by and clear to the data subject. This can be mapped to our taxonomy as shown in Table 3.

Miyazaki et al. [18] propose the Privacy Requirements Elicitation Technique (PRET). The authors derived 35 privacy requirements from different sources. They built a tool that assists requirements engineers to identify the relevant privacy requirements based on a questionnaire. Unfortunately, the authors do not provide the full list of privacy requirements, only a list of 11 privacy requirements is presented. The list includes two relevant requirements. Data subjects shall be informed about the purpose of data processing and they shall be notified about personal data breaches. These requirements can be mapped to our taxonomy as shown in Table 3.

Feigenbaum et al. [11] investigated privacy engineering for digital rights management systems. For this they adopted the fair information principles to digital rights management systems. The principle *collection limitation* needs to inform data subjects about the purpose of data collection. The principle *purpose disclosure (notice)* stresses that information provided to data subjects has to be easily understandable. These principles can be mapped to our taxonomy as shown in Table 3.

Pötzsch [21] proposes requirements on transparency enhancing tools. The author states that these tools shall inform data subjects about which personal data flows to whom and for which purpose it is processed in way that it is understandable, tailored to the specific situation, and does not decrease the performance of the tool. This can be mapped to our taxonomy as shown in Table 3.

Wicker and Schrader [25] introduce five privacy-aware design principles for information networks. The principles *provide full disclosure of data collection* is concerned with providing data subjects with all relevant information about how the data is processed in a way that is understandable by the user. This principle can be mapped to our taxonomy as shown in Table 3.

Kung et al. [15] restate transparency as: *"applications should be designed and operated so that maximum transparency can be provided to stakeholders on the way privacy preservation is ensured."*. This can be mapped to our taxonomy as shown in Table 3.

Langheinrich [16] investigated which principles have to be considered for a privacy-aware development of ubiquitous systems. One of these principles is *Notice* and concerned with providing users adequate information about the collection of personal data. This principle can be mapped to our taxonomy as shown in Table 3.

3.2 Privacy Policies and Obligations

Lobato et al. [33] present 7 patterns for privacy policies. The goal of the pattern *Privacy Policy Definition* is *"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."*. The pattern *Privacy Policy Issues* stresses the need to inform data subjects about security mechanisms, people who have access to their data, the choices the data subject has concerning the processing. According to the pattern *Notification of Risks and Changes*, users have to be notified as soon as a change occurs. This corresponds to a case of our exceptional information requirement. The pattern *Personal Information Objectives* suggest to inform data subjects about the purpose and reasons for the collected data. These patterns can be mapped to our taxonomy as shown in Table 4.

Antón et al. [27,28,29] derived from around 50 web site privacy policies in the e-commerce and health domain a privacy goal and a vulnerability taxonomy. These taxonomies shall help consumers to compare different web site privacy policies and to decide which web site provides the privacy protection fitting to their needs. Antón and Earp identified the transparency related goals *General Notice/Awareness*, *Identification of the uses to which the data will be put*, *Identification of any potential recipients of the data*, *Nature of the data collected*, *Steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data*, *Choice of how data is used*, *Choice of sharing data*, and *Choice of what data is taken/stored*. Table 4 shows which requirements of our taxonomy address these goals.

Casassa Mont [30] presents a technical framework to handle privacy obligations. The author defines several requirements a privacy obligation handling framework has to address. These requirements include the definition of the data related to the obligation and of the person who is responsible for the enforcement of the obligation, the need to track changes in obligations, present data subjects their rights, and how their data is used in a well understandable way. This can be mapped to our taxonomy as shown in Table 4.

Alcade Bagüés et al. [26] present an architecture for a privacy management system based on privacy obligations. The authors define seven types of notification obligations. The type *access* is concerned with notifications about the purpose and changes of it when data is accessed, *leaking* is concerned with informing about data breaches, *disclosure* with describing to whom personal data flows, *repository* with informing about the data stored, *deletion* with notification when data is removed, and *policy* with the notification of changes in the privacy policy. These obligations can be mapped to our taxonomy as shown in Table 4.

Kelley et al. [31,32] propose a *"privacy nutrition label"* to visualize P3P[2] privacy policies in a way that they are easier to understand for data subjects. The nutrition label contains (such as P3P) the information which types of information is how used and shared with whom. Additionally, it contains the information whether there is a opt-in or opt-out option for the user to restrict the data usage. This can be mapped to our taxonomy as shown in Table 4.

3.3 Empirical Research on User's Privacy Awareness

Sheth et al. [35] performed an empirical study on privacy requirements across North America, Asia, and Europe. The summarized their results into a privacy framework consisting of 7 *"qualities and features"* namely, *Anonymization*, *Data usage*, *Default encryption*, *Fine-grained control over the data*, *Interaction data first*, *Time and space-limited storage*, and *Privacy, policies, laws, and usage details*. The quality *Data usage* aims at providing data usage details to data subjects and to *"make these more transparent and easier to understand"*. The quality *Time and space-limited storage* requires to inform data subjects about the duration and location of data storage and flow. This is reflected in our taxonomy in the storage and flow information requirements.

Reinfelder et al. [34] performed a study on the differences between Android and iPhone user's security and privacy awareness. They conclude that apps shall provide a clear overview of the data accessed by them to data subjects. This can be mapped to our taxonomy as shown in Table 4.

Zviran [36] studied the correlation of online user's privacy concerns based on the five dimensions of privacy concerns proposed by Sheehan and Hoy [37]. The concern *awareness of information collection* shall be addressed by informing data subjects about the collection of personal data. The concern *information usage* adds the need to inform data subjects about the purposes for which the data is used. These concerns can be mapped to our taxonomy as shown in Table 4.

3.4 Privacy from the Legal Perspective

Solove [44] a taxonomy of privacy violations which is not limited to information systems. Three of these violations contain hints on needs to inform data subjects. From the violation *exclusion* we can conduct that data subjects have to be informed about which personal data is processed and for which purpose. From *breach of confidentiality*, we can conduct that data subjects have to be informed, if a breach of their personal data occurred. And from *disclosure*, we can conduct that data subjects have to be informed to whom information is disclosed, this can relate to the normal behavior and also to data breaches.

Van der Sype and Seigneur [45] analyzed the legal requirements for the use of social login features on the basis of the Belgian implementation of the EU legal framework on

[2] `http://www.w3.org/P3P/`

privacy and data protection. As we used the EU legal framework to derive our taxonomy, we did not find any additional transparency requirements in their work.

Mulligan [41] and Wright [42] suggest privacy impact assessments (PIAs) as a tool to provide transparency to data subjects. The information needed for a PIA report includes information about the processor, the personal data collected and processed, the information flows.

Jones and Tahri [40] derived from EU law the information that has to be presented to website visitors. They have identified three categories of information that has to be provided. *Information about website operator* corresponds to the controller in our terminology, *information about marketing/selling activities* includes the notification about the data subject's right to withdraw consent, and *information about processing of personal data/data privacy* is concerned with informing the data subject about the purpose of data processing. This can be mapped to our taxonomy as shown in Table 4.

Breaux and Gordon [38] compare the needs to inform about data breaches in different US states. Tomaszewski [39] also discusses the needs to inform about data breaches and provides a list of information that has to be provided to data subjects and authorities in the case of a data breach. This list can be used to enhance the attributes of our exceptional information requirement.

Otto et al. [43] analyzed a data breach at the data broker ChoicePoint and derived some recommendations for data brokers. The recommendations that are relevant for transparency are the following. *Provide prompt and accurate notification* recommends to provide consistent information to the involved data subjects and authorities as soon as possible. *Express the company's overall privacy practices clearly* recommends to inform about the security mechanisms the controller has in place to protect the personal data, the choices the data subject has on how his/her data is processed, and to whom the data flows. These recommendations can be mapped to our taxonomy as shown in Table 4.

Wright and Raab [46] criticize that the privacy principles proposed by ISO/IEC 29100 only address four of seven types of privacy that where identified by Finn et al.[50]. To cover all types of privacy Wright and Raab suggest nine additional principles of which two contain transparency requirements. The principle *right to autonomy* implies that data subjects have to be informed about indirect data collection. The principle *right not to have to pay in order to exercise privacy rights* implies that the information about the management of personal data has to be accessable for data subjects free of charge. These principles can be mapped to our taxonomy as shown in Table 4.

From Table 3 and Table 4, we can see that almost all papers in the category *Privacy (Requirements) Engineering* have considered *what* information has to be provided to data subjects, but only the halve of these papers mentioned that it is important *how* this information is provided. Only three contained aspects related to notification of data subjects in exceptional cases, e.g., data breaches. Note that none of the papers in this category covered all elements of our taxonomy. The papers in the category *Empirical Research on Privacy Awareness* mainly investigate the users' awareness of data processing. The papers did not give recommendations on how data subjects shall be informed about exceptional cases. In the category *Privacy from the Legal Perspective*, we have papers that consider single laws or aspects that can be reflected by single elements of our taxonomy, and papers that consider a larger legal framework or privacy impact assessments and hence, cover (almost) all elements of our taxonomy. The papers in the category *Privacy Policies and Obligations* provide the most structured, detailed, and complete concepts related to transparency requirements. Nevertheless, we did not find any literature that provides an as structured, detailed, and complete overview of transparency requirements as our proposed taxonomy shown in Fig. 2.

4 Conclusions

This technical report presents the details of the literature review performed for the research paper [1]. In our research, 1) we systematically derived requirements for the privacy goal transparency from the ISO/IEC 29100:2011 standard [4] and the draft of the EU Data Protection Regulation [5]. These two documents belong to the most relevant sources for privacy requirements that have to be considered by software developers. 2) We then structured these requirements in a metamodel for transparency requirements. This metamodel provides an overview of the identified kinds of transparency requirements and shall help requirements engineers to identify and document the transparency requirements relevant for them and the information needed to address the transparency requirements. 3) We performed a systematic literature review and provide an overview of the relevant research related to transparency requirements. 4) We validated that our taxonomy contains all necessary aspects mentioned in the identified literature. The literature review showed that all aspects of the privacy goal transparency mentioned in the literature are reflected in the proposed taxonomy. Furthermore, we did not find any literature that presents transparency requirements in an as structured, detailed, and complete manner. Our proposed metamodel of the taxonomy can easily be adopted and extended.

As future work, we plan to develop a systematic process that assists requirements engineers to identify the relevant transparency requirements based on a given set of functional requirements. Furthermore, we will develop a tool to generate human-readable representations of the instantiated transparency requirements of our proposed metamodel based on text templates.

References

1. Meis, R., Wirtz, R., Heisel, M.: A taxonomy of requirements for the privacy goal transparency. In: Trust, Privacy, and Security in Digital Business. LNCS, Springer (2015)
2. Hansen, M.: Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In: Privacy and Identity Management for Life. IFIP AICT 375. Springer (2012) 14–31
3. Probst, T., Hansen, M.: Privacy protection goals in privacy and data protection evaluations. Working paper, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (July 2013)
4. ISO/IEC: ISO/IEC 29100:2011 Information technology – Security techniques – Privacy Framework. Technical report, International Organization for Standardization and International Electrotechnical Commission (2011)

5. European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (January 2012) `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011`.
6. OECD: OECD guidelines on the protection of privacy and transborder flows of personal data. Technical report, Organisation of Economic Co-Operation and Development (1980)
7. US Federal Trade Commission: Privacy online: Fair information practices in the electronic marketplace, a report to congress (2000)
8. Solovo, D., Rotenberg, M.: Information privacy law. Aspen elective series. Aspen Publishers (2003)
9. Breaux, T.: Privacy requirements in an age of increased sharing. Software, IEEE **31**(5) (Sept 2014) 24–27
10. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. RE (2011)
11. Feigenbaum, J., Freedman, M., Sander, T., Shostack, A.: Privacy engineering for digital rights management systems. In: Security and Privacy in Digital Rights Management. LNCS 2320. Springer (2002) 76–105
12. Fhom, H., Bayarou, K.: Towards a holistic privacy engineering approach for smart grid systems. In: IEEE 10th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom). (Nov 2011) 234–241
13. Hedbom, H.: A survey on transparency tools for enhancing privacy. In: The Future of Identity in the Information Society. IFIP AICT 298. Springer (2009) 67–82
14. Hoepman, J.: Privacy design strategies - (extended abstract). In: ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC. IFIP AICT 428, Springer (2014) 446–459
15. Kung, A., Freytag, J.C., Kargl, F.: Privacy-by-design in its applications. In: IEEE Int. Symp. on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). (June 2011) 1–6
16. Langheinrich, M.: Privacy by design — principles of privacy-aware ubiquitous systems. In: Ubiquitous Computing (Ubicomp). LNCS 2201. Springer (2001) 273–291
17. Masiello, B.: Deconstructing the privacy experience. Security Privacy, IEEE **7**(4) (July 2009) 68–70
18. Miyazaki, S., Mead, N., Zhan, J.: Computer-aided privacy requirements elicitation technique. In: IEEE Asia-Pacific Services Computing Conf. (APSCC). (Dec 2008) 367–372
19. Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S.: A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software **86**(9) (2013) 2276 – 2293
20. Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., Kavakli, E.: Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces **36**(4) (2014) 759 – 775
21. Pötzsch, S.: Privacy awareness: A means to solve the privacy paradox? In: The Future of Identity in the Information Society. IFIP AICT 298. Springer (2009) 226–236
22. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit - DuD **33**(6) (2009) 353–358
23. Bier, C.: How usage control and provenance tracking get together - a data protection perspective. In: IEEE Security and Privacy Workshops (SPW). (May 2013) 13–17
24. Spiekermann, S., Cranor, L.: Engineering privacy. Software Engineering, IEEE Transactions on **35**(1) (Jan 2009) 67–82
25. Wicker, S., Schrader, D.: Privacy-aware design principles for information networks. Proceedings of the IEEE **99**(2) (Feb 2011) 330–350

26. Alcalde Bagüés, S., Mitic, J., Zeidler, A., Tejada, M., Matias, I., Fernandez Valdivielso, C.: Obligations: Building a bridge between personal and enterprise privacy in pervasive computing. In: Trust, Privacy and Security in Digital Business. LNCS 5185. Springer (2008) 173–184
27. Antón, A.I., Earp, J.B., Reese, A.: Analyzing website privacy requirements using a privacy goal taxonomy. In: IEEE Int. Conf. on Requirements Engineering. (2002) 23–31
28. Antón, A.I., Earp: A requirements taxonomy for reducing web site privacy vulnerabilities. Requirements Engineering **9**(3) (2004) 169–185
29. Anton, A., Earp, J., Vail, M., Jain, N., Gheen, C., Frink, J.: HIPAA's effect on web site privacy policies. Security Privacy, IEEE **5**(1) (Jan 2007) 45–52
30. Casassa Mont, M.: Dealing with privacy obligations: Important aspects and technical approaches. In: Trust and Privacy in Digital Business. LNCS 3184. Springer (2004) 120–131
31. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A "nutrition label" for privacy. In: Proc. of the 5th Symp. on Usable Privacy and Security. SOUPS '09, ACM (2009) 4:1–4:12
32. Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F.: Standardizing privacy notices: An online study of the nutrition label approach. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. CHI '10, ACM (2010) 1573–1582
33. Lobato, L., Fernandez, E., Zorzo, S.: Patterns to support the development of privacy policies. In: Int. Conf. on Availability, Reliability and Security (ARES). (March 2009) 744–749
34. Reinfelder, L., Benenson, Z., Gassmann, F.: Differences between Android and iPhone users in their security and privacy awareness. In: Trust, Privacy, and Security in Digital Business. LNCS 8647. Springer (2014) 156–167
35. Sheth, S., Kaiser, G., Maalej, W.: Us and them: A study of privacy requirements across North America, Asia, and Europe. In: Proc. of the 36th Int. Conf. on Software Engineering. ICSE 2014, ACM (2014) 859–870
36. Zviran, M.: User's perspectives on privacy in web-based applications. Journal of Computer Information Systems **48**(4) (2008) 97–105
37. Sheehan, K.B., Hoy, M.G.: Dimensions of privacy concern among online consumers. Journal of Public Policy & Marketing **19**(1) (2000) 62–73
38. Breaux, T., Gordon, D.: What engineers should know about us security and privacy law. Security Privacy, IEEE **11**(3) (May 2013) 72–76
39. Tomaszewski, J.: Are you sure you had a privacy incident? Security Privacy, IEEE **4**(6) (Nov 2006) 64–66
40. Jones, R., Tahri, D.: EU law requirements to provide information to website visitors. Computer Law & Security Review **26**(6) (2010) 613 – 620
41. Mulligan, D.: The enduring importance of transparency. Security Privacy, IEEE **12**(3) (May 2014) 61–65
42. Wright, D.: The state of the art in privacy impact assessment. Computer Law & Security Review **28**(1) (2012) 54 – 61
43. Otto, P., Anton, A., Baumer, D.: The ChoicePoint dilemma: How data brokers should handle the privacy of personal information. Security Privacy, IEEE **5**(5) (Sept 2007) 15–23
44. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania Law Review **154**(3) (Januar 2006) 477–560
45. Sype, Y.S.V.D., Seigneur, J.: Case study: legal requirements for the use of social login features for online reputation updates. In Cho, Y., Shin, S.Y., Kim, S., Hung, C., Hong, J., eds.: Symposium on Applied Computing, SAC, ACM (2014) 1698–1705
46. Wright, D., Raab, C.: Privacy principles, risks and harms. International Review of Law, Computers & Technology **28**(3) (2014) 277–298
47. Jalali, S., Wohlin, C.: Systematic literature studies: Database searches vs. backward snowballing. In: Proc. of the ACM-IEEE Int. Symp. on Empirical Software Engineering and Measurement. ESEM 2012, ACM (2012) 29–38

48. Howard, M., Lipner, S.: The Security Development Lifecycle. Microsoft Press, Redmond, WA, USA (2006)
49. European Parliament: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (October 1995) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.
50. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y., eds.: European Data Protection: Coming of Age. Springer (2013) 3–32

Table 4. Detailed mapping of transparency notions from the literature to our proposed taxonomy - Part 2

Privacy Policies and Obligations

Source	Mentioned Concept	PR	EIR	PIR	SIR	FIR	CIR
Alcade Bagüés et al. [26]	Access		X	X			
	Leaking		X				
	Disclosure					X	
	Repository				X		
	Deletion				X		
	Policy		X				
Antón et al. [27,28,29]	General Notice/Awareness	X	X	X			X
	Identification of the uses to which the data will be put			X	X	X	
	Identification of any potential recipients of the data					X	
	Nature of the data collected						X
	Steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data		X	X			
	Choice of how data is used			X			
	Choice of sharing data			X		X	X
	Choice of what data is taken/stored			X	X		X
Casassa Mont [30]	Modelling and representation of privacy obligations			X			
	Tracking the evolutions of obligation policies		X				
	User involvement	X		X	X	X	X
Kelley et al. [31,32]	Privacy Nutration Label	X		X		X	
Lobato et al. [33]	Privacy Policy Definition	X		X	X	X	X
	Privacy Policy Issues			X	X	X	X
	Notification of Risks and Changes		X				
	Personal Information Objectives			X	X	X	X

Empirical Research on User's Privacy Awareness

Source	Mentioned Concept	PR	EIR	PIR	SIR	FIR	CIR
Reinfelder et al. [34]	Overview of data accessed by app			X	X		X
Sheth et al. [35]	Data usage	X		X	X	X	X
	Time and space-limited storage				X	X	
Zviran [36], Sheehan et al. [37]	Awareness of Information Collection						X
	Information Usage			X			

Privacy from the Legal Perspective

Source	Mentioned Concept	PR	EIR	PIR	SIR	FIR	CIR
Breaux and Gordon [38], Tomaszewski [39]	Data breaches		X				
Jones and Tahri [40]	Information about website operator			X			
	Information about marketing/selling activities			X			
	Information about processing of personal data/data privacy			X			
Mulligan [41], Wright [42]	PIA Report	X			X	X	X
Otto et al. [43]	Provide prompt and accurate notification	X	X				
	Express the company's overall privacy practices clearly			X	X	X	X
Solove [44]	Exclusion			X			
	Breach of Confidentiality		X				
	Disclosure		X			X	
Van der Sype and Seigneur [45]	Legal requirements	X	X	X	X	X	X
Wright and Raab [46]	Right to autonomy						X
	Right not to have to pay to exercise privacy rights	X					

PR: PresentationRequirement, **EIR**: ExceptionalInformationRequirement,**PIR**: ProcessingInformationRequirement, **SIR**: StorgeInformationRequirement, **FIR**: FlowInformationRequirement, **CIR**: CollectionInformationRequirement