Understanding the Privacy Goal Intervenability

Rene Meis(✉) and Maritta Heisel

paluno - The Ruhr Institute for Software Technology,
University of Duisburg-Essen, Duisburg, Germany
{rene.meis,maritta.heisel}@paluno.uni-due.de

Abstract. Privacy is gaining more and more attention in society and hence, gains more importance as a software quality that has to be considered during software development. A privacy goal that has not yet been deeply studied is the empowerment of end-users to have control over how their personal data is processed by information systems. This privacy goal is called intervenability. Several surveys have shown that one of end-users' main privacy concerns is the lack of intervenability options in information systems. In this paper, we refine the privacy goal intervenability into a software requirements taxonomy and relate it to a taxonomy of transparency requirements because transparency can be regarded as a prerequisite for intervenability. The combined taxonomy of intervenability and transparency requirements shall guide requirements engineers to identify the intervenability requirements relevant for the system they consider. We validated the completeness of our taxonomy by comparing it to the relevant literature that we derived based on a systematic literature review.

1 Introduction

A central concern of end-users with regard to privacy is that they have almost no control over their personal data once these are put into an information system [1–4]. End-users wish for more empowerment, i.e. they want to keep the control over their personal data and how their data is processed by information systems. Hansen [5] summarizes this and other privacy needs into the privacy goal *intervenability*. Hansen states *"Intervenability aims at the possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing. The objective of intervenability is the application of corrective measures and counterbalances where necessary."* [5].

Intervenability is a complex software quality that is strongly coupled with other privacy-related goals. For example, end-users have to be sufficiently aware of how and what personal data is processed and which options exist to intervene in order to be able to exercise these options. Hence, the privacy goal transparency can be seen as prerequisite for intervenability.

This work was partially supported by the Deutsche Forschungsgemeinschaft (DFG) under grant No. GRK 2167, Research Training Group "User-Centered Social Media".

S. Katsikas et al. (Eds.): TrustBus 2016, LNCS 9830, pp. 79–94, 2016.
DOI: 10.1007/978-3-319-44341-6_6

As a first step to assist requirements engineers to deal with the complex privacy goal intervenability, we propose a requirements taxonomy that further refines intervenability into subrequirements enriched with attributes and associated to transparency requirements that we identified in [6]. The taxonomy shall help requirements engineers to understand which intervenability and transparency requirements have to be considered for the system they analyze.

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

2 Deriving and Structuring Requirements on Intervenability

In Sect. 2.1, we systematically analyze the privacy principles described by the international standard ISO/IEC 29100:2011 [7] and the draft of the EU data protection regulation [8] to derive the intervenability requirements they contain and the transparency requirements related to them. To derive the requirements, we analyze the description of the privacy principles and the formulations of the regulation. We keep the formulation of the identified intervenability and transparency requirements close to the original documents from which we identified them. In Sect. 2.1, we enumerate these derived requirements using the notation I*n* for intervenability requirements and T*n* for the related transparency requirements. 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 an intervenability requirement In_1 refines a part of another requirement In_2, this means that In_1 adds further details on how or which possibilities have to exist to intervene in the processing of personal data. Furthermore, we identified that there are transparency requirements that are closely related to intervenability requirements. This is, because in order to be able to make use of intervenability mechanisms, data subjects have to be aware of them. Hence, we use a *relatedTo* relation to make the relations between transparency and intervenability requirements explicit. The *refines* (directed dashed edges) and *relatedTo* (solid edges) relation are visualized as an initial overview of intervenability requirements in Fig. 1. In Sect. 2.2, we structure the intervenability requirements identified in Sect. 2.1 into a taxonomy of intervenability requirements and integrate this taxonomy into the taxonomy of transparency requirements introduced in [6]. The taxonomy is presented as an extensible metamodel using a UML class diagram.

ISO/IEC 29100:2011 and the draft of the EU data protection regulation do not use the same terminology. To avoid ambiguities, we 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, [...].” This term is called *PII principal* in ISO/IEC 29100:2011.

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; [...].”* This term is called *PII controller* in ISO/IEC 29100:2011.

Supervisory authority *“means a public authority which is established by a Member State in accordance with Article 46.”* Article 46 states that supervisory authorities *“are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, [...].”*

2.1 Requirements Identification from Privacy Principles and Legislation

ISO/IEC 29100 Privacy Principles. To derive our taxonomy of intervenability requirements, we first consider the international standard ISO/IEC 29100:2011 [7], which defines 11 privacy principles which are a superset of the OECD principles [9] and the US fair information practices (FIPs) [10].

We start our analysis with the *consent and choice principle*, which is obviously concerned with providing data subjects the power to decide how their data is processed. From this principle, we obtain the following intervenability and transparency requirements.

I1 Present to the data subjects the choice whether or not to allow the processing of their personal data.

I2 Obtain the opt-in consent of the data subject for collecting or otherwise processing sensitive personal data.

T1 Inform data subjects before obtaining consent about their rights to access their personal data and to influence the processing of these.

I3 Provide data subjects with the opportunity to choose how their personal data is handled.

I4 Allow data subjects to withdraw consent easily and free of charge.

T2 Where the personal data processing is not based on consent but instead on another legal basis, the data subject should be notified wherever possible.

I5 Where the data subject has the ability to withdraw consent and has chosen to do so, these personal data should be exempted from processing for any purpose not legally mandated.

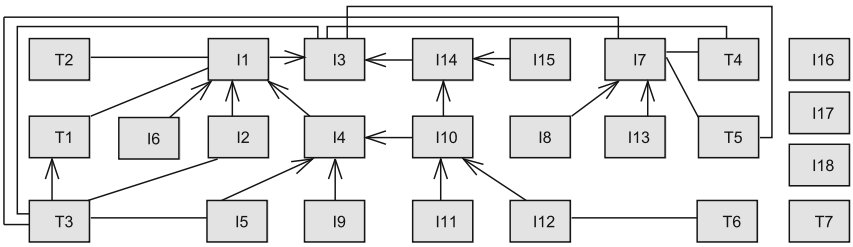

Fig. 1. Initial overview of intervenability requirements

I6 Provide data subjects with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their personal data at the time of collection, first use or as soon as practicable thereafter.

Requirement I3 states that data subjects shall have the opportunity to choose how their data is handled and is the most general intervenability requirement. It is refined by I1 (cf. Fig. 1) that states that data subjects shall have the choice whether their data is processed or not. I1 is further refined by I2 that requires opt-in consent for processing of sensitive personal data, I4 that requires the possibility to withdraw consent, and I6 that describes requirements for the mechanisms to realize I1. I5 refines I4 by describing the effects of withdrawing consent. Both transparency requirements T1 and T2 are related to I1 (cf. Fig. 1). T1 requires that data subjects have to be informed about their rights before consent is obtained. T2 requires to inform data subjects if their data is processed without their explicit consent.

From the *openness, transparency and notice principle* we identify an additional transparency requirement that is related to all intervenability requirements that describe the choices and means for data subjects to influence how their data is processed (cf. Fig. 1).

T3 Disclose the choices and means offered by the controller to data subjects for the purposes of limiting the processing of, and for accessing, correcting and removing their information.

The following two intervenability requirements are derived from the *individual participation and access principle*.

I7 Give data subjects the ability to access and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law.

I8 Allow data subjects to challenge the accuracy and completeness of their personal data and have it amended, corrected or removed as appropriate and possible in the specific context.

I7 and I8 are not refinements of the already identified intervenability requirements, because they are not concerned with how data subjects can influence

how or if their personal data is processed. But we consider I8 as a kind of refinement of I7, because I8 depends on I7. Note that I7 prescribes that data subjects shall be empowered with the ability to access and review their personal data. Hence, I7 is considered as an intervenability requirement. Nevertheless, allowing data subjects to access and review their personal data also contributes to transparency.

The other principles presented in ISO 29100 do not contain further statements from which we can derive intervenability requirements.

Draft of the EU Data Protection Regulation. To identify further intervenability and transparency requirements and to refine the already identified requirements, we analyze the draft of the EU data protection regulation[1] [8]. We selected this regulation as a representative data protection regulation. In contrast to the situation in the US where no privacy regulations covering all industrial branches exist, the EU data protection regulation covers all industrial branches.

Article 7 describes the conditions for consent and we derive from it the following intervenability requirement that refines I4.

I9 The data subject shall have the right to withdraw his or her consent at any time.

Article 12 specifies requirements on mechanisms for exercising the rights of data subjects. We identified the following two transparency requirements that are related to all intervenability requirements that describe the choices and means for data subjects to influence how their data is processed.

T4 The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken if a data subject requested information and shall provide the requested information.

T5 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.

Article 17 is about the right to be forgotten and to erasure. From this article we derive the following requirements.

I10 The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data if the data subject withdraws consent or objects to the processing of personal data.

[1] The draft of the EU data protection regulation was adopted with some changes on 27 April 2016 and entered into force on 24 May 2016. Note that our analysis is based on the draft and not on the final version of the regulation.

I11 The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary.
I12 Where erasure is not possible, the controller shall instead restrict processing of personal data.
T6 The controller shall inform the data subject before lifting the restriction on processing.

I10, I11, and I12 refine the consequence of withdrawing consent (I4) and objecting to processing (I14 see below). T6 requires that data subjects are informed about the restrictions on processing implied by I12 before these are lifted.

The right to data portability is introduced by Article 18. It implies the following intervenability requirement that refines I7.

I13 The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

Article 19 describes the right to object. From this we derived the following two intervenability requirements that refine I3.

I14 The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data, unless the controller demonstrates compelling legitimate grounds for the processing.
I15 If the objection is valid, the controller shall no longer use or otherwise process the personal data concerned.

Article 53 describes the powers of supervisory authorities. In contrast to the previously identified requirements, the following requirements do not describe intervention possibilities for data subjects or needs to provide information to data subjects, but for/to supervisory authorities.

T7 Supervisory authorities may order the controller to provide any information relevant for the performance of their duties to them.
I16 Supervisory authorities may order the rectification or erasure of all data when they have been processed in breach of the provisions of a regulation.
I17 Supervisory authorities may impose a temporary or definitive ban on processing.
I18 Supervisory authorities may order to suspend data flows to a recipient in a third country or to an international organization.

Table 1 summarizes from which ISO 29100 principles and articles of the draft of the EU data protection regulation which initial intervenability and transparency requirements were derived. Additionally, it allows to associate the elements of our intervenability requirements taxonomy (introduced in the next section) with the principles and articles from which these were identified.

Table 1. Mapping of ISO principles and data protection articles to the requirements

Principle/Article	I*n*/T*n*	IR	DIR	AIR	PIR	EIR	IIR
Consent and choice	I1–I6, T1, T2	X	X		X		
Openness, transparency and notice	T3		X		X		
Individual participation and access	I7, I8	X	X				
Article 7	I9		X				
Article 12	T4, T5						X
Article 17	I10–I12, T6	X	X				X
Article 18	I13	X	X				
Article 19	I14, I15	X	X				
Article 53	I16–I18, T7	X		X		X	

IR: IntervenabilityRequirement DIR: DataSubjectInterventionRequirement
AIR: AuthorityInterventionRequirement PIR: ProcessingInformationRequirement
EIR: ExceptionalInformationRequirement IIR: InterventionInformationRequirement

2.2 Setting up an Intervenability Requirements Taxonomy

We now structure the identified preliminary intervenability requirements into an intervenability requirements taxonomy. We integrate this taxonomy into the transparency requirements taxonomy presented in earlier work [6] using the related preliminary transparency requirements. Figure 2 shows our taxonomy in the form of a metamodel using a UML class diagram. Note that we only show the attributes and enumerations of the transparency taxonomy that are relevant for this paper. All elements that have bold font and thick lines are newly added to the transparency taxonomy. The requirements with dark gray background represent the newly identified transparency and intervenability requirements.

Table 2 provides an overview of how the initial requirements are reflected in our proposed taxonomy. In the following, we explain the new elements of our taxonomy and how they are related to the requirements introduced in [6].

Intervenability Requirement. The root element of our intervenability requirements taxonomy is the *IntervenabilityRequirement*. We modeled it as an abstract class because only its specializations shall be instantiated. It contains the attribute effect that describes the consequences of an intervenability requirement. The possible effects are derived from the preliminary requirements I1, I3, I5, I7, I8, I10–I13, and I15–I18, and are summarized in the enumeration InterventionEffect (cf. Fig. 2). The effects are that data subjects get *access* to their personal data, that their personal data is *not processed*, that the *processing is restricted*, that their personal data is *amended*, *corrected*, or *erased*, that they *receive a copy* of their data, and that *data flows are suspended*. In addition to the effect that an intervenability requirement shall have, it has a type describing how data subjects or supervisory authorities can cause the wanted effects. As these

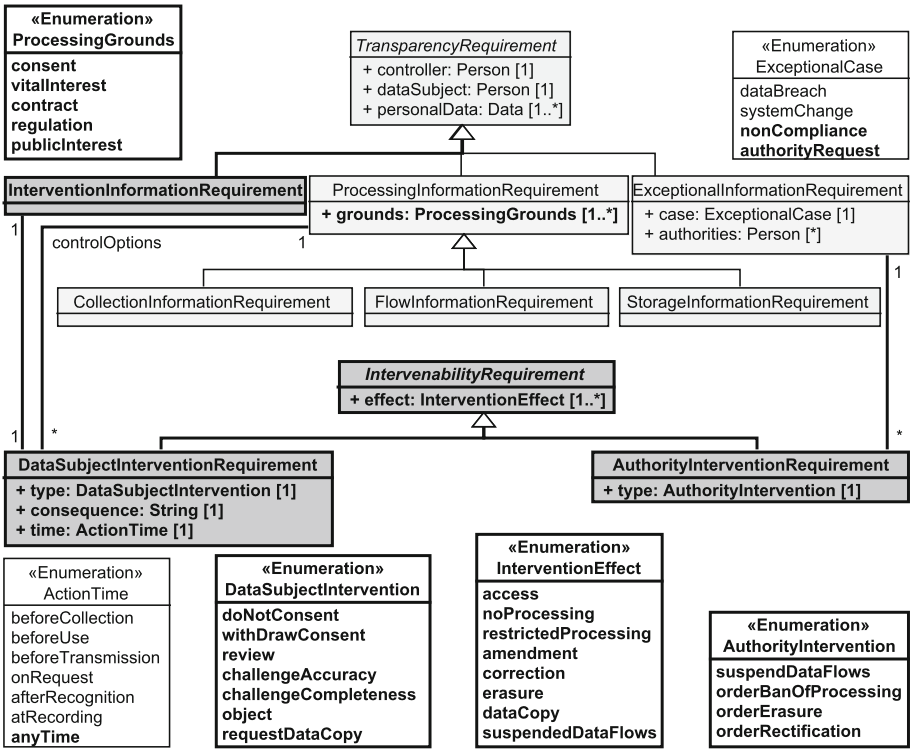

Fig. 2. Our combined taxonomy of transparency and intervenability requirements.

Table 2. Mapping between taxonomy and preliminary requirements

Requirement	Attribute	In/Tn
IntervenabilityRequirement	effect	I1, I3, I5, I7, I8, I10–I13, I15–I18
DataSubjectInterventionRequirement	type	I1–I5, I7, I8, I10–I15
	time	I6, I9, I14
	consequences	T1, T3, I6
AuthorityInterventionRequirement	type	I16, I17, I18
ProcessingInformationRequirement	controlOptions	T1, T3, I6
	grounds	T2
ExceptionalInformationRequirement	exceptionalCase	I16, I17, I18, T7
InterventionInformationRequirement		T4, T5, T6

Table 3. Mapping between authority intervention types and intervention effects

Intervention Type	Possible Intervention Effects	Source
suspendDataFlows	suspendedDataFlows	I18
orderBanOfProcessing	noProcessing, restrictedProcessing	I17
orderErasure	erasure	I16
orderRectification	correction, amendment	I16

types differ for data subjects and authorities, we added the attribute type to the intervenability requirements DataSubjectInterventionRequirement (representing intervention possibilities for data subjects) and AuthorityInterventionRequirement (representing intervention possibilities for supervisory authorities).

AuthorityInterventionRequirement. Almost all initial requirements describe rights of data subjects to influence how their personal data is processed. Only I16, I17, I18, and T7 present possibilities for supervisory authorities to intervene in the processing of personal data. The intervention types for authorities are summarized in the enumeration AuthorityIntervention (cf. Fig. 2). Supervisory authorities may order to *suspend data flows*, order a *ban of processing* of personal data, and order the *erasure* or *rectification* of personal data. The initial requirements I16, I17, and I18 also describe which type of intervention shall lead to which kind of intervention effect. Hence, there are limitations for the combination of intervention types and effects when an ExceptionalInformationRequirement is instantiated. Table 3 presents the valid combinations of intervention types and effects.

T7 indicates that supervisory authorities have to be informed about the processing in order to exercise their rights to intervention properly. Hence, each AuthorityInterventionRequirement has an ExceptionalInformationRequirement assigned that describes which supervisory authorities may intervene. We newly introduced into the enumeration ExceptionalCase the literals nonCompliance and authorityRequest to reflect that authorities have to be informed in the case of processing of personal data in a way that does *not comply* with the regulations and that authorities then have the possibility to intervene in this processing. Additionally, authorities have the right to *request* information concerning the processing of personal data from the controller.

DataSubjectInterventionRequirement. The DataSubjectInterventionRequirement presents the possibilities for data subjects to intervene in the processing of their personal data. These possibilities are summarized in the enumeration DataSubjectIntervention (cf. Fig. 2) that we derived from the preliminary requirements I1–I5, I7, I8, and I10–I15. These initial requirements additionally describe which combinations of intervention types and effects are allowed for DataSubjectInterventionRequirements. The valid combinations are shown in Table 4.

T1, T3, I6, and I9 require that data subjects have to be informed about how they can intervene in the processing of their personal data. To reflect this, we introduced the association controlOptions between DataSubjectInterventionRequirement and ProcessingInformationRequirement (cf. Fig. 2). From the

Table 4. Mapping between data subject intervention types and intervention effects

Intervention Type	Possible Intervention Effects	Source
doNotConsent	noProcessing	I2
withDrawConsent	noProcessing, restrictedProcessing, erasure	I4, I5, I10, I12
review	access	I7
challengeAccuracy	correction, amendment, erasure	I8
challengeCompleteness	amendment, erasure	I8
object	noProcessing, restrictedProcessing, erasure	I10, I12, I15
requestDataCopy	dataCopy	I13

perspective of the ProcessingInformationRequirement, the association describes which options exist for data subjects to intervene in the processing of their personal data. The two attributes consequence and time of DataSubjectInterventionRequirement are used to describe further details on the control option described by the DataSubjectInterventionRequirement. The attribute consequences allows to provide a textual description of the consequences that the utilization of the corresponding intervenability option has. The attribute time describes when data subjects can exercise the corresponding option.

From the preliminary requirements T4–T6, we identified that an additional transparency requirement should be added to the taxonomy. This requirement states the need to inform data subjects about the progress or rejection of interventions requested by them. For this purpose, we introduce the InterventionInformationRequirement. Each DataSubjectInterventionRequirement is associated to an InterventionInformationRequirement and vice versa that presents the need to inform data subjects about the progress or rejection of their intervention.

Furthermore, we identified from T2 that the ProcessingInformationRequirement should also inform data subjects about the legal grounds on which their data is processed. For this, we enriched this requirement with an attribute grounds that reflects the possible grounds for processing personal data by the controller. These are derived from ISO 29100 and the draft of the EU data protection regulation. They are *consent* of the data subject, the *vital interest* of the data subject, an existing *contract*, a *regulation* that allows the processing, and *public interest*.

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 intervenability. 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 intervenability concepts used in the literature.

To identify the relevant related work, we performed a systematic literature review using backward snowballing [11]. To obtain the starting set of papers for

our review, we manually searched the proceedings and issues of the last 10 years of computer science 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[2] ranking. In this way, we selected 15 conferences and 19 journals. First, we checked whether title or abstract of a paper indicates that the paper is concerned with privacy (requirements), intervenability, empowerment, user's controls, or user's choices. In this way, we obtained 219 articles. We then analyzed the full texts of these articles. Doing this, we reduced the number of relevant articles to 21. Due to the manual search process, we have to deal with the threat to validity that our starting set of papers does not contain all relevant literature, because it was published in a source that we did not consider or was published earlier than in the last 10 years. To mitigate this threat, we applied backward snowballing. That is, we also considered the papers referenced in the papers that we identified as relevant until no new candidates were found. During the snowballing, we identified 79 possibly relevant articles from which 12 were finally considered as relevant. In total, we identified 298 papers that seemed to be relevant after reading title and abstract. After the analysis of the full text, we finally identified 33 papers as related work. Due to space limitations, we cannot present all details of the literature review in this paper, but we provide an overview of our key findings.

The most important finding is that we are able to map each explicitly mentioned intervenability-related concept in the literature to an element of our taxonomy and that none of the articles provides such a structured overview of intervenability requirements and relates these explicitly to transparency requirements. Table 5 shows to which degree the articles identified during the literature review address the intervenability requirements that we identified in this work. For each article, we investigated to which degree aspects of the DataSubjectInterventionRequirement (column **DIR**), the AuthorityInterventionRequirement (column **AIR**), and the relations between intervenability and transparency requirements (column **RIT**) are mentioned in it. We distinguish in Table 5 three cases. If all aspects are addressed, we denote this with a "+". If the aspects are only partially considered, then we denote this with a "o". If no aspects are addressed, we denote this with a "−".

From Table 5, we can see that no article discusses all aspects concerning the relation between intervenability and transparency requirements. Several papers mention that transparency is a prerequisite for intervenability or that data subjects have to be aware of their options to intervene in the processing of their personal data, but none of the papers mentioned that data subjects have to be informed about the progress of the intervention requests they have triggered. Few of the articles considered the intervention options of supervisory authorities. Only three articles covered all of the aspects and 5 identified the need to be able to answer requests of supervisory authorities in order to prove compliance with regulations or standards. All articles discuss at least partially options for the data subject to intervene into the processing of their personal data. The most

[2] http://www.core.edu.au/conference-portal (accessed on 20 June 2016).

Table 5. Mapping of intervenability notions from the literature to our taxonomy

Source	DIR	AIR	RIT
Bier [12], Hansen [5]	+	+	o
Hoepman [13]	+	o	o
Mouratidis et al. [14]	o	o	o
Miyazaki et al. [15]	+	+	–
Kalloniatis et al. [16,17], Spiekermann and Cranor [18]	o	o	–
Makri and Lambrinoudakis [19], Acquisti et al. [20], Masiello [21], Krol and Preibusch [22], Deng et al. [23], Komanduri et al. [24], Cranor [25], Wicker and Schrader [26]	o	–	o
Strickland and Hunt [27], Sheth et al. [28], Fhom and Bayarou [29], Antón et al. [30,31], Van der Sype and Seigneur [32], Basso et al. [33]	+	–	–
Lobato et al. [34], Caron et al. [35], Zuiderveen Borgesius [36], Breaux [37], Langheinrich [38], Feigenbaum et al. [39], Wright and Raab [40], Guarda and Zannone [41], Hedbom [42], Smith et al. [43]	o	–	–

DIR: DataSubjectInterventionRequirement, AIR: AuthorityInterventionRequirement
RIT: Relation between intervenability and transparency requirements

often discussed intervenability option is to consent or withdraw consent. Another interesting observation that we made is that only Hoepman [13] discusses the right to data portability. This right, its implementation, and consequences seem to not yet have been discussed deeply in the literature.

4 Conclusions

In this paper, (1) we systematically derived requirements for the privacy goal intervenability and related transparency requirements from the ISO 29100 standard [7] and the draft of the EU data protection regulation [8]. (2) We then integrated these requirements into an existing metamodel for transparency requirements [6]. The new metamodel provides an overview of the identified kinds of transparency and intervenability requirements and how these are related to each other. The metamodel shall furthermore help requirements engineers to identify and document the transparency and intervenability requirements relevant for them and the information needed to address the transparency and intervenability requirements. (3) We performed a systematic literature review and provide an overview of the relevant research related to intervenability 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 intervenability mentioned in the literature are reflected in the proposed taxonomy. Furthermore, we did not find any literature that presents

intervenability requirements and their relation to transparency requirements in such a structured, detailed, and complete manner.

We believe that our taxonomy is flexible enough to also represent intervenability and transparency requirements from other regulations and standards, because our proposed metamodel of the taxonomy can easily be adopted and extended. In these cases our metamodel can be enhanced with, e.g., further intervention types and effects. These can easily be added to the corresponding enumerations (cf. Fig. 2).

For future research, we identified three open research questions. (1) How can the taxonomy be used to derive intervenability requirements for a specific software to be developed? To answer this question, we want to integrate the intervenability requirements and their relations to the transparency requirements into our method for the automatic identification and validation of privacy requirements [44]. (2) Which kinds of threats to transparency and intervenability requirements exist? (3) Which technologies exist that implement transparency and intervenability requirements or mitigate threats to these? To address the latter two questions, we plan to set up a catalog of threats that possibly lead to a violation of the identified transparency and intervenability requirements and related mechanisms that may be used to mitigate the identified threats. Based on this catalog, we want to develop a systematic method to identify the relevant threats for a given set of functional requirements and appropriate countermeasures in order to perform a privacy risk assessment.

Acknowledgment. We thank Sylbie Sabit who provided a starting point for this research with her master thesis [45].

References

1. GSMA: MOBILE PRIVACY: consumer research insights and considerations for policymakers, February 2014. http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf. Accessed 20 June 2016
2. Symantec: State of Privacy Report 2015 (2015). https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf. Accessed 20 June 2016
3. Quah, A.M.Y., Röhm, U.: User awareness and policy compliance of data privacy in cloud computing. In: Proceedings of the First Australasian Web Conference, AWC 2013, vol. 144, pp. 3–12, Darlinghurst, Australia, Australian Computer Society, Inc. (2013)
4. Ackerman, M.S., Cranor, L.F., Reagle, J.: Privacy in e-Commerce: examining user scenarios and privacy preferences. In: Proceedings of the 1st ACM Conference on Electronic Commerce, EC 1999, New York, NY, USA, pp. 1–8. ACM (1999)
5. Hansen, M.: Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity Management for Life. IFIP AICT, vol. 375, pp. 14–31. Springer, Heidelberg (2012)

6. Meis, R., Wirtz, R., Heisel, M.: A taxonomy of requirements for the privacy goal transparency. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.) TrustBus 2015. LNCS, vol. 9264, pp. 195–209. Springer, Heidelberg (2015)
7. ISO/IEC: ISO/IEC 29100:2011 Information technology - Security techniques - Privacy Framework. Technical report, International Organization for Standardization and International Electrotechnical Commission (2011)
8. 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). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011. Accessed 20 June 2016
9. OECD: OECD guidelines on the protection of privacy and transborder flows of personal data. Technical report, Organisation of Economic Co-Operation and Development (1980)
10. US Federal Trade Commission: Privacy online: Fair information practices in the electronic marketplace, a report to congress (2000)
11. Jalali, S., Wohlin, C.: Systematic literature studies: database searches vs. backward snowballing. In: Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2012, pp. 29–38. ACM (2012)
12. Bier, C.: How usage control and provenance tracking get together - a data protection perspective. In: IEEE Security and Privacy Workshops (SPW), pp. 13–17, May 2013
13. Hoepman, J.: Privacy design strategies - (extended abstract). In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., El Kalam, A.A., Sans, T. (eds.) ICT Systems Security and Privacy Protection. IFIP Advances in Information and Communication Technology, vol. 428, pp. 446–459. Springer, Heidelberg (2014)
14. Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S.: A framework to support selection of cloud providers based on security and privacy requirements. J. Syst. Softw. **86**(9), 2276–2293 (2013)
15. Miyazaki, S., Mead, N., Zhan, J.: Computer-aided privacy requirements elicitation technique. In: IEEE Asia-Pacific Services Computing Conference (APSCC), pp. 367–372, December 2008
16. 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. Comput. Stand. Interfaces **36**(4), 759–775 (2014)
17. Kalloniatis, C.: Designing privacy-aware systems in the cloud. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.) TrustBus 2015. LNCS, vol. 9264, pp. 113–123. Springer, Heidelberg (2015)
18. Spiekermann, S., Cranor, L.: Engineering privacy. IEEE Trans. Softw. Eng. **35**(1), 67–82 (2009)
19. Makri, E.-L., Lambrinoudakis, C.: Privacy principles: towards a common privacy audit methodology. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.) TrustBus 2015. LNCS, vol. 9264, pp. 219–234. Springer, Heidelberg (2015)
20. Acquisti, A., Adjerid, I., Brandimarte, L.: Gone in 15 seconds: the limits of privacy transparency and control. IEEE Secur. Priv. **11**(4), 72–74 (2013)
21. Masiello, B.: Deconstructing the privacy experience. IEEE Secur. Priv. **7**(4), 68–70 (2009)
22. Krol, K., Preibusch, S.: Effortless privacy negotiations. IEEE Secur. Priv. **13**(3), 88–91 (2015)

23. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. RE **16**, 3–32 (2011)
24. Komanduri, S., Shay, R., Norcie, G., Ur, B., Cranor, L.F.: Adchoices? compliance with online behavioral advertising notice and choice requirements. Technical report, CyLab - Carnegie Mellon University (2011). https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf. Accessed 20 June 2016
25. Cranor, L.F.: Necessary but not sufficient: standardized mechanisms for privacy notice and choice. JTHTL **10**(2), 273–308 (2012)
26. Wicker, S., Schrader, D.: Privacy-aware design principles for information networks. Proc. IEEE **99**(2), 330–350 (2011)
27. Strickland, L.S., Hunt, L.E.: Technology, security, and individual privacy: new tools, new threats, and new public perceptions: research articles. J. Am. Soc. Inf. Sci. Technol. **56**(3), 221–234 (2005)
28. Sheth, S., Kaiser, G., Maalej, W.: Us and them: a study of privacy requirements across North America, Asia, and Europe. In: Proceedings of the 36th International Conference on Software Engineering, ICSE 2014, pp. 859–870. ACM (2014)
29. Fhom, H., Bayarou, K.: Towards a holistic privacy engineering approach for smart grid systems. In: IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 234–241, November 2011
30. Antón, A.I., Earp, J.B., Reese, A.: Analyzing website privacy requirements using a privacy goal taxonomy. In: IEEE International Confernce on Requirements Engineering, pp. 23–31 (2002)
31. Antón, A.I.: Earp: a requirements taxonomy for reducing web site privacy vulnerabilities. Requirements Eng. **9**(3), 169–185 (2004)
32. 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, pp. 1698–1705. ACM (2014)
33. Basso, T., Moraes, R., Jino, M., Vieira, M.: Requirements, design and evaluation of a privacy reference architecture for web applications and services. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing, pp. 1425–1432. ACM (2015)
34. Lobato, L., Fernandez, E., Zorzo, S.: Patterns to support the development of privacy policies. In: International Conference on Availability, Reliability and Security (ARES), pp. 744–749, March 2009
35. Caron, X., Bosua, R., Maynard, S.B., Ahmad, A.: The internet of things (iot) and its impact on individual privacy: an Australian perspective. Comput. Law Secur. Rev. **32**(1), 4–15 (2016)
36. Borgesius, F.Z.: Informed consent: we can do better to defend privacy. IEEE Secur. Priv. **13**(2), 103–107 (2015)
37. Breaux, T.: Privacy requirements in an age of increased sharing. IEEE Softw. **31**(5), 24–27 (2014)
38. Langheinrich, M.: Privacy by design — principles of privacy-aware ubiquitous systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) UbiComp 2001. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001)
39. Feigenbaum, J., Freedman, M.J., Sander, T., Shostack, A.: Privacy engineering for digital rights management systems. In: Sander, T. (ed.) DRM 2001. LNCS, vol. 2320, pp. 76–105. Springer, Heidelberg (2002)
40. Wright, D., Raab, C.: Privacy principles, risks and harms. Int. Rev. Law, Comput. Technol. **28**(3), 277–298 (2014)

41. Guarda, P., Zannone, N.: Towards the development of privacy-aware systems. Inf. Softw. Technol. **51**(2), 337–350 (2009)
42. Hedbom, H.: A survey on transparency tools for enhancing privacy. In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) The Future of Identity. IFIP AICT, vol. 298, pp. 67–82. Springer, Heidelberg (2009)
43. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. MIS Q. **35**(4), 989–1016 (2011)
44. Meis, R., Heisel, M.: Computer-aided identification and validation of privacy requirements. Information **7**(2), 28 (2016)
45. Sabit, S.: Consideration of intervenability requirements in software development. Master thesis, University of Duisburg-Essen, Germany, August 2015