IOP Publishing

Human-Assisted Intelligent Computing

Modeling, simulations and applications

Mukhdeep Singh Manshahia, Igor S Litvinchev, Gerhard-Wilhelm Weber, J Joshua Thomas and Pandian Vasant

Chapter 6

Computing the intelligent privacy-engineered organization: a metamodel of effective information transparency enhancing tools/technologies

Ljerka Luic and Marta Alic

In information privacy research, privacy is described as a set of system properties. Such properties are formalized as technical functionalities in ensuring data subjects' rights in knowing what data is being collected and processed about them and what they have control over. To ensure this, transparency enhancing tools/technologies (TETs) are used to enhance understanding and visibility of procedures, practices and consequences of personal data processing with data processors. As a combination of technological and organizational solutions or methods their goals can be perceived as privacy, as well as a software engineering prerequisite. Since the principles of data privacy are the subject of numerous international documents from the 1970s, with different levels of abstraction, methods of goal-based reasoning can be applied in their requirement analysis. By using identification, classification and modelling heuristics of the Goal-Based Requirement Analysis Method, requirements for effective TETs are systemized across momentous Data Privacy Governance Frameworks. The synthesis made of relevant transparency goals can serve as a precondition for computing intelligent privacy organizational environments.

6.1 Introduction

In today's age of information abundance, privacy is becoming a luxury. Activities that have been private until recently are now becoming a source of profit by analyzing the interests, characteristics, beliefs, worldviews and intentions of individuals. Using numerous internet services, users, consciously but also unconsciously,

doi:10.1088/978-0-7503-4801-0ch6

share numerous data to various stakeholders: among themselves, to organizations and public authorities.

The issue of privacy is becoming more expressed as is the ability of individuals to control their data in intelligent system environments. Advances in information technology have made the collection and the use of personal data invisible. As a result, individuals rarely have a clear knowledge of what information others have about them or how that information is used and with what consequences.

Although the systems of modern, digital economy are based on an exchange of data for the benefit of all stakeholders as well as society as a whole, the possibilities of data misuse, such as discrimination [1, 2] and manipulation, are alarming, and research shows and considers individuals an important factor in online decision-making [3]. The report of the research project Horizon 2020 of the European Union [4] related to privacy on the platforms of so-called economy sharing shows that service providers mostly express some concern about the misuse of their data as well as the loss of control over their online presentation due to the negative reviews or comments from other users. In fact, the whole concept of so-called impression management, the strategic sharing of personal data to create a more affordable online view, is a source of anxiety for users.

To meet user requirements and design systems according to the Privacy by Design concept, which focuses on system engineering that puts privacy in focus throughout the system design process [5], organizations need to implement high standards of privacy throughout the organizational system and business culture, including visibility and transparency, as a key precondition for ensuring the right of individuals to privacy.

However, in the field of requirement engineering within information systems, transparency is a relatively new topic. The reason is that the concept was approached primarily from the perspective of software engineering and only then the design of the entire information system, in which transparency was usually categorized as a non-functional requirement in relation to software functionality, considered primarily as a 'second-rate' quality issue [6].

The first research in the field of requirement engineering suggested the application of the so-called non-functional requirement (NFR) framework [7] and method of i* modelling [8], allowing for these not to be the final solutions. Further research has led to the definition of aspects of transparency [9], a concept that contains the following five NFRs: accessibility, usability, information, comprehensibility and auditability as conditions for achieving transparency. Furthermore, focused on user requirements are two papers by Dabbish *et al* [10, 11], who cite Github as an example of a transparent software environment, bringing it into relationship with the paradigm of openness of social networks, while [12] at the same time suggesting the application of the so-called argumentation framework in meeting user transparency requirements in software engineering.

Finally, noticing the gap in related literature in the field of transparency requirements from a user or data subject perspective, following their previous research [13, 14], Hosseini *et al* developed a modelling language [15] and, consequently, set up conceptual models [16] in relation to business information systems.

The objective of this chapter is to provide a comprehensive review of requirement engineering goals for effective transparency tools or technology modelling and development, set by the data governance frameworks in the field of privacy. Section 6.2 first provides background material on TETs in the context of privacy management as well as an overview of data privacy governance frameworks and their development. In section 6.3 the selected frameworks are put into an interrelationship, resulting in derived transparency requirements, their entity-relationship metamodel and goal-driven taxonomy. Section 6.4 discusses analysed governance frameworks in the context of their historic development and their relations to current regulatory and standard privacy practices. Section 6.5 refers to the major findings and limitations of the research in reference to the goal-based requirements analysis method. Section 6.6 concludes the chapter, eliciting future scope of the research.

6.2 Transparency enhancing tools/technologies

6.2.1 Right to privacy and information transparency

The right to privacy is a fundamental human right, both international and constitutional, which protects a person from excessive encroachment of state power, the public and other individuals into an individual's spatial and informational intimacy. Different dimensions of privacy, from spatial and physical, privacy of communication to information privacy, can therefore be studied in the so-called vertical relationship to the institutions of the state and society or horizontal relationship to third parties, while their boundaries are constantly reviewed and revised, depending on the context or social and civilizational environment. Accordingly, the right to privacy is not an absolute right, and it is accomplished in addition to the rights of others to know the necessary information about individuals.

Data privacy is a form of material privacy based on the right and ability of an individual to define and live their life in a way determined by themselves [17] in relation to data created by themselves or by others, by observation and analysis, consumption or processing. That kind of data is called personal information (PI). Confidentiality, the ability to choose with whom (or what) to share the information about oneself is one aspect of privacy, while anonymity and de-identification, the separation of information from the subject to which it might otherwise relate [18], are other aspects.

So, the concept of data privacy can be defined as authorized, fair and legitimate processing of personal information where an individual to whom the data applies, or a data subject (who is literally the subject matter of the information) is the ultimate requirement-setting entity. But for the data subject to be able to make informed decisions and have control over his/her privacy, it is necessary for data controllers (the natural or legal persons, public authorities, agencies or other bodies) to provide quality transparency tools, designed to provide insight into data processing practices and their consequences.

In today's human-computer interaction (HCI) environments, the relation between users and services that collect users' information is characterized by high information asymmetry [19]. So, it is a great imperative that people obtain the

correct mental models regarding the flow of their personal data. TETs are methods or tools which enhance transparency and can provide users with more control over their PI. TETs can be considered as tools that provide insight into the method the personal data is collected, stored, processed and disclosed in an accurate and comprehensible way [20].

As measures for privacy protection, TETs are generally seen as a combination of technological solutions and legal or procedural frameworks and diverse classifications of TETs can be made based on the degree of interactivity and intervention provided to data subjects [21], their execution environments [22], assertions or declarations by data processors [21] and other parameters. An important distinction for transparency tools is the division into ex-ante (inform before processing), ex-post (inspect after processing) and real-time (inform while processing) TETs [21].

The way data controllers address and implement privacy requirements is an individual decision, as data privacy is a key part of data governance in organisations. In this context, privacy engineering is the construction of data governance into the design and implementation of routines, systems and products that process PI [23]. Privacy frameworks and guidelines can navigate in creating the necessary roles and responsibilities needed to build and maintain privacy-aware enterprises. They are used as tools to recognize and understand privacy policies at meta-use-case requirements for privacy engineering.

6.2.2 Data privacy governance frameworks overview

The Organisation for Economic Co-operation and Development (OECD) Guidelines [24] are one of the better-known privacy governance frameworks as an extension of a series of principles called the Fair Information Practice Principles (FIPPs) [25], developed by the Department of Health, Education, and Welfare in the 1960s in reaction to concerns over implementation of large government databases containing information on citizens of the United States of America. The principles were extended by the OECD in 1980 in a document titled 'The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'. These principles have become the foundation for the majority of the existing privacy laws and regulations.

It was a regulatory motive for this document in the first place, as OECD Member countries considered it necessary, due to the development of automatic data processing, to develop guidelines which would help to harmonise national privacy legislation and, while upholding human rights on privacy, would at the same time prevent interruptions in international flows of data [24]. As a result, the document represents unanimity on the basic principles which can be integrated into existing national legislation, or serve as a basis for developing legislation in countries which do not have it yet.

The same efforts in the development of effective privacy protection that avoid barriers to information flow and ensure continued trade and economic growth in the Asia-Pacific region were made by the development of The Asia-Pacific Economic Cooperation (APEC) Privacy Framework [26]. It is in line with and also models the

core values of the OECD Guidelines on Privacy and Cross-Border Personal Data Flows and reaffirms the value of privacy for individuals and the information society.

The National Institute of Standards and Technology (NIST) Privacy Framework [27] is focused on deriving benefits from the data, while simultaneously managing risks to individuals' privacy. It follows the structure of The Framework for Improving Critical Infrastructure Cybersecurity [28] and is composed of three parts: Core, profiles, and implementation tiers, where each component reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities. By focusing more on the development of practical privacy engineering requirements, rather than on the general principles recognized in OECD and APEC documents, it sets out a precise overview of activities and outcomes that enable a dialogue on privacy risk management, such as GAPP (Generally Accepted Privacy Principles) [29], developed by the American Institute of Chartered Accountants (AICPA) and the Working Party on Privacy of the Canadian Institute of Chartered Accountants (CICA), to address business perspectives and address significant local, national and international privacy regulations.

GAPP, on the other hand, operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by an objective, measurable criterion that forms the basis for effective management of privacy risk and compliance in an organization [23].

6.3 Modelling effective transparency enhancing tools/technologies

6.3.1 Aligning privacy frameworks in transparency

The process of requirement engineering consists of determining user needs or expectations in modelling new solutions. In this context, a solution is manifested in an effective TET, characterized by the quantifiable, relevant and detailed requirements. In software engineering such requirements are often called functional specifications and the same development path can be used for requirement gathering and development in privacy engineering. After all, privacy policy creation serves as a critical requirement gathering source or end state upon which to draw certain functional requirements of a system.

For privacy engineers, requirement gathering and development can follow the same development journey as any other functional specifications, but with a variation. The mastery of privacy policy creation for the enterprise is often stated in aspirational or behavioral terms: reasonable, proportional, 'do no harm' options and choices but in TET context policy it serves as a critical requirement-gathering source or end state upon which certain functional requirements for privacy enhancing environments are drawn.

So, to derive the transparency goals related to transparency tools, the description of the privacy principles and their formulations was analysed across all presented privacy frameworks. As transparency is an inevitable part of privacy engineering, all privacy engineering frameworks align with it, albeit with a different terminology (table 6.1).

Table 6.1. Alignment of privacy frameworks in transparency terminology.

NIST Privacy Framework [27]	OECD Guidelines [24]	APEC Privacy Framework [26]	GAPP [29]
Data processing awareness	Specification of purpose	Notice	Notice

The most general goal for information transparency is set as a specification of purpose principle in the OECD guidelines: 'The purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose', which provides guidance regarding the type and quality of transparency or respective tools, setting the first categorization criteria for requirement engineering.

The concept of transparency implies two dimensions: visibility, i.e. the degree of completeness of information and the possibility of finding it, and inferability, the degree to which information can be used to make the right decisions [30]. So, effective transparency tools should aim at meeting a high degree of both dimensions of transparency to ensure that information asymmetry is reduced, ensuring a multi-faceted means for 'providing necessary information', as the first and 'providing quality mechanisms', as the second initial or root factor. This is also recognized by APEC, which has set out in more detail the principle of privacy of notification notices, referring to the availability and comprehensibility of data processing statements, as well as the main requirements in informativeness, ie. the transfer of good quality information.

Transparency prerequisites and requirements in the NIST privacy framework are targeted as a data processing awareness category in the communicate function section of the document, generally defined as a rule that 'individuals and organizations have reliable knowledge of data processing practices and associated privacy risks', implying that mechanisms for communicating this knowledge are established and in place.

For these principles, in the GAPP measurement criteria are presented in more detail, giving the most detailed set of requirements in privacy engineering. Notice principle, defined in a separate section as prerequisite in privacy policies, extends its criteria also to other principles describing more detailed requirements for achieving transparency goals.

6.3.2 Transparency requirements mining

In the detailed requirement-mining process from framework documents the formulation of the identified requirements was kept close to the original documents to ease the overlap distinguishment. Some of the requirements represent a refinement of another requirement, adding further details on how (applying 'providing quality mechanisms' factor, noted with M) or which possibilities have to exist (applying 'providing necessary information' factor, noted with I) in order to maximize the quality of information transparency.

The analysis started with provide notice principle as root principle of providing information about policies and procedures (I1), following principles related to the mechanism requirements regarding the notice.

I1 Provide notice about privacy policies and procedures [27].

M1 Provide clear and easily accessible notices about practices and policies with respect to personal information [26].

M2 Provide notice at the time of, or before information about them is collected [24, 26].

M3 Notice is conspicuous and uses plain and simple language [29].

M4 Notice is appropriately labelled and easy to use [29].

Requirements M1 and M2 are the refinement of the principle requirement I1 providing more specific demands on the notice such as a place (where it should be provided) and time (when notice should be provided). By defining the notice criteria as easily accessible, it is suggested that transparency should be attained considering best media for notice dissemination. This requirement can be further refined with M4, as transparency increases with appropriate label of notice and simplicity in use and endorsed with M3 that emphasizes the demand of visibility and details the ease of use with a plain and simple language requirement.

Providing information of data processing purpose is a principle used to define transparency requirements of informativeness, starting with I2 as the most generic one.

I2 Identify the purposes for which personal information is collected, used, retained and disclosed [24, 26, 29].

I3 Describe the personal information collected, sources and methods used to collect it and purposes for which it is collected [29].

I4 Provide the purpose for collecting sensitive personal information (if applicable) and whether such purpose is part of a legal requirement [29].

I5 Inform data subjects that information is collected only for the purposes identified in the notice [29].

I6 Inform that personal information not essential to the purposes need not be provided [29].

I7 Describe the consequences, if any, of not providing the requested information [29].

I2 defines the data processing activities (collection, usage, retention and disclosure) across the information flow and I3 is the refinement of the collection phase. I4 places emphasis on providing explanations whenever sensitive data is used and hence refines the previous requirement I3.

As the purpose of data processing is the key element of transparency, on which data subjects can base their decision about (not) sharing their personal data, requirements I5–I7 explicitly mandate that.

I12 Indicate that certain information about individuals may be developed [29].

I12 is another refinement of I2 considering that collection of information is not strictly constricted directly from the first party but, considering contemporary technology, it can be aggregated from other sources.

I10 Describe the practices relating to sharing of personal information (if any) with third parties and the reasons for information sharing [29].
I11 Identify third parties or classes of third parties to whom personal information is disclosed [29].

I10 and I11 reference disclosure phase of data flow, while I11 is a detailed refinement of I10.

I15 Provide information that personal information is retained for no longer than necessary to fulfil the stated purposes or for a period specifically required by law or regulation [29].
I16 Provide information that personal information is disposed of in a manner that prevents loss, theft, misuse or unauthorized access [29].
I17 Inform about precautions taken to protect personal information [29].
I18 Describe the general types of security measures used to protect personal information [29].

I15 and I16 focus on the retention phase of the data flow and disposal of data, while I17 and I18 refer to security measures applied.

Finally, the principle of user control and participation in data processing derived requirements that can emancipate user intervenability and contribution.

I8 Inform that implicit or explicit consent is required to collect, use and disclose personal information, unless a law or a regulation specifically requires or allows otherwise [29].
I9 Inform that preferences may be changed and consent may be withdrawn at a later time, subject to legal or contractual restrictions and a reasonable notice [29].

Consent is a major principle in data processing legitimacy. If there isn't any regulatory legal basis for collecting, using and disclosing personal information that would imply implicit consent, it is required for the data controller to ensure an explicit one and inform the user about that (I8) as well as to imply that consent is not indefinite, but subject to change (I9). In terms of explicitness, the quality of being clear and exact in consenting, I9 is a refinement of I8.

I14 Notice is clearly dated to allow individuals to determine whether it has changed since the last time they read it or since the last time they submitted their personal information to the entity [29].

To address currentness of notice, requirement I14 is defined to improve transparency.

I13 Provide information about the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information [29].

I13 is a prerequisite requirement for intervenability of data subjects that can be refined with succeeding requirements.

I20 Explain how disagreements related to personal information may be resolved [29].

I21 Provide information about choices and means available for limiting the use and disclosure of personal information, accessing and correcting them [29].
I22 Explain the process of how the data subject may gain access to personal information and any cost associated with gaining such access [29].
I23 Outline the means by which data subjects may update and correct their personal information [29].

6.3.3 Transparency requirements metamodel

The structure of identified transparency requirements for effective TETs can be modelled by using a UML class diagram (figure 6.1). Requirements are mapped to reflect their relations, using standardized notation to signal the relationship strength, mutual association and/or dependence.

6.3.4 Transparency requirements classification

Developing from the described relations in figure 6.1, metamodel, requirements can be mapped in taxonomy, showed in table 6.2, according to the goals they achieve. In

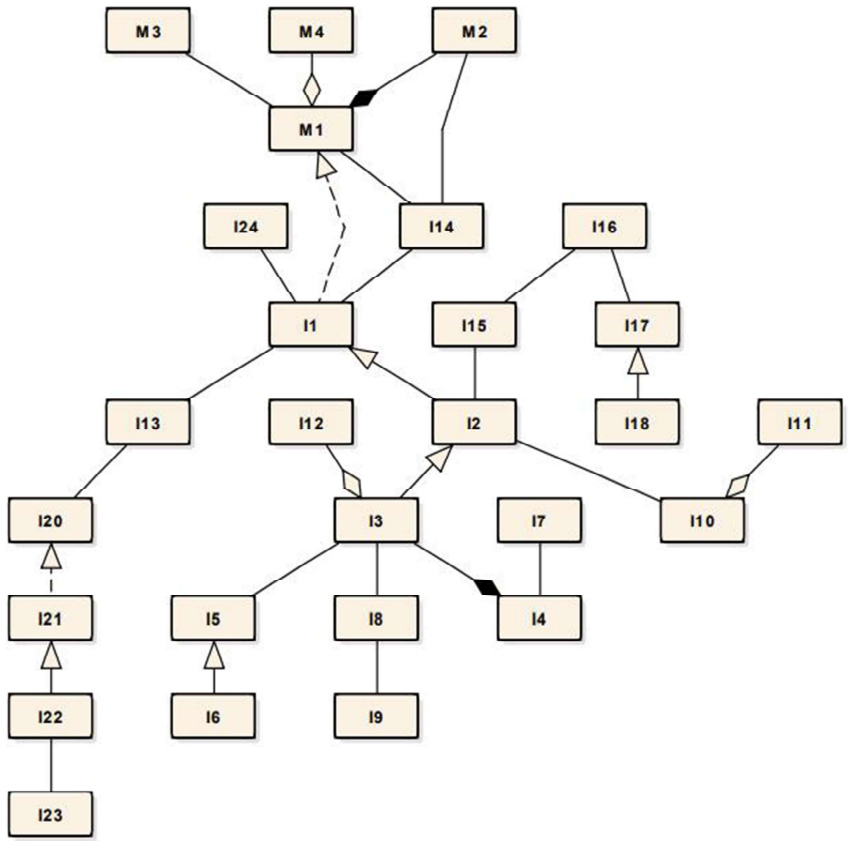

Figure 6.1. A metamodel of TET requirements.

Table 6.2. Alignment of privacy frameworks in transparency terminology.

Goal	Attribute	
Transparency	notice	I1, I14
	controller	I13
	legal	I8, I9
Mechanism	mechanism	M1–M4
Processing	purpose	I2, I4, I5, I6
	collection	I3, I12
	retention	I15, I16
	disclosure	I10, I11
	security	I16, I17, I18
Control	choice	I14, I20, I21
	information quality	I22, I23

requirements engineering, the goal-driven approaches focus on why the systems are constructed, expressing the rationale and justification for the proposed system [31]. To 'target' them more specifically to the operationalization goals of the system, requirements are further classified by attributes.

On the top-level element of hierarchy there is the general transparency goal which corresponds to the initial requirement I1. It has three attributes that instantiate requirements more specifically. The attribute notice relates to requirements that are related to the notice itself—its existence (I1) and its currentness or accuracy in providing information about the real process of the system (I14). I14 is an informativeness requirement as it provides the date of notice as a criterion establishing the currentness of the document, as opposed to other possible methods of stating accuracy of notice within the mechanisms of media (for example, setting automatic date of publishing the document on electronic media). The Controller attribute is used to single out the requirement about the personal data controller, their identity, location and contact information (I13). Lastly, to separate requirements which are contextual to legal regulations, attribute legal is used. If a legal basis for data processing is consent, it is required to inform the data subjects about that (I8), as well as mention 'conditions' of such consent (I9). In the model, these instances are associated to more generalized I3 which describes methods, sources and collected information specifying how it can be used by data subjects for decision-making about (non)consenting to the data processing.

To address requirements which are subject to mechanism qualities, mechanism goal is defined with instances, accordingly annotated, from M1 to M4. As appropriate labelling of mechanism (M4) is a prerequisite for providing 'easily accessible notices' (M1) the relationship is defined as an aggregation to indicate that labelling is a part of privacy notices. Composition, a stronger form of association is used to define the relationship between M1 and M2 which defines the timeliness of the notice as an important part of transparency that refers to the time expected for accessibility and availability of information. Finally, comprehensibility of the language for the targeted audience is required in order for it to enhance transparency

by using 'plain and simple language' (M3) which is associated with the mechanism quality.

The processing goal presents requirements grounded in I2 and contains properties of data processing practices and its purposes along the data flow. It has five attributes, with the purpose attribute used to provide a set of statements (I4 to I6) that could consist of declarative requirements: fulfilment of what cause the personal data of the data subject is needed for. It is also considered in the I3 requirement, as its specialization within the collection requirements. Since providing purpose for collecting sensitive information is a conditional instance and it is only required if applicable, so I4 is set as a composition of I3—collection description, while I5 and I6 are more specialized instances of I2 and I3 as a proxy requirement. I12 describes collection methods in case certain information may be developed about individuals and, as such, it is aggregated part of I3.

The retention attribute represents requirements which inform the data subject about the set retention periods and criteria for its determination (I15) as well as methods of its disposal 'in a manner that prevents loss, theft, misuse or unauthorized access' (I16). The means described in I16 are related also to the security requirements investigated by I17—to 'inform about precautions taken to protect personal information' and I18 as its more specialized requirement of describing data security types of measures. And although these requirements are not part of the data flow, security is its integral part and an inevitable layer in privacy engineering, so its requirements are attributed accordingly and put under the processing goal.

The requirements of control goal are essential to managing the data subject's rights. They are represented with the choice and information quality attributes. Although I14 requirement, which says that 'notice is clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity' is subject to transparency goal, it can also be a decisive element for the data subject consent, therefore it is also sorted under the choice cohort, alongside requirements I20 'explain how disagreements related to the personal information may be resolved' and providing 'information about choices and means available for limiting the use and disclosure of personal information, accessing and correcting them' (I21), where I21 can be interpreted as a realization of I20.

To distinguish the more specific requirements to I21, an information quality attribute is introduced to refine requirements I22 and I23 as detailed representations of explaining 'the process of how the data subject may gain access to the personal information and any cost associated with gaining such access' and 'the means by which data subjects may update and correct their personal information'.

6.4 Leveraging privacy principles

Since the appearance of the General Data Protection Regulation (GDPR) [32] in European Union (EU) member countries, the majority of privacy engineering literature has focused on explaining requirements aligned with this legislative document.

But privacy engineering, voluntary or regulatory, is not a new concept. The Council of Europe's 1981 Convention has had a greater influence than the OECD Guidelines

in the legislation of the European Union Member States. It has continued in the EU's data protection Directive 95/46/EC which has now been superseded by the GDPR. With minor, but important changes of wording, the Directive replicated the Convention Articles and added important changes of wording, as the Directive depicted the Convention Articles, adding further rules about the legitimacy of processing and the transfer of personal data to third countries [33].

Meanwhile, as OECD guidelines have become globally very influential, which is reflected in the countries' adoption of their own data protection legislation, it was the report from United States of America's Federal Trade Commission in 1998 that led to modernization of privacy endeavours. By having reduced prior collections of principles down to five, it stated that most of them, except for security, are procedural, as substantive obligations concerning fairness and data quality were ignored in favour of procedural requirements concerning notice, choice, access and enforcement.

It was the APEC Privacy Framework in 2005 that put a conscious effort into building on the OECD guidelines and modernizing them, escalating demand for standards that facilitate multinational data flows [34].

While the numbers and formulations of the principles vary in compliance frameworks, a consensus has existed since the 1970s. Any public or private organization that deals with PI should be accountable for all of the PI in its possession. It should also identify the purposes for which the information is processed at or before the time of collection. Data gathering should also be processed lawfully and transparently by collecting only PI with the knowledge and consent of the individual (except under specified circumstances). The collection of PI should be limited to what is necessary for pursuing the identified purposes and collected personal data should not be used or disclosed for purposes other than those identified (except with the individual's consent). Information should be retained only as long as necessary; while ensuring that PI is kept accurate, complete, up to date and protected with appropriate security safeguards. Organizations also need to be transparent about their policies and practices and maintain no secret information systems, allowing the data subjects access to their PI, with an ability to amend it if it is inaccurate, incomplete or obsolete [33].

But the most significant privacy protection 'textbook' is an ISO 29100 international standard for privacy principles, published by the International Organization for Standardization in 2011, deriving from the existing principles developed by various states, countries and international organizations. These standards for voluntary compliance are defined in 11 privacy principles which are a superset of the OECD principles and the US fair information practices (FIPs).

6.5 Research findings and limitations within the scope of the goal-based requirements analysis method

6.5.1 Major research findings and contributions

Since privacy goals in all frameworks are evolutionary, they provide a common language for all participants in the process, regardless of whether they observe them from the technical and/or organizational perspective.

The Goal-Based Requirement Analysis Method (GBRAM) [31, 35] is a straightforward methodical approach in identifying and refining the goals that software systems must achieve, converting them into operational requirements. As transparency is one notion of privacy management, it is generally perceived simply as a notice about data governing practices, but, as a derived taxonomy clearly shows, tools for ensuring effective transparency require quality of mechanism properties to be assured. And this is, in most cases within contemporary environment of digital economy, a functional requirement of engineering software systems.

The GBRAM method suggests goal identification and refinement strategies and techniques through the inclusion of a set of heuristics as a form of knowledge and reasoning: identification heuristics, classification heuristics, refinement heuristics, elaboration heuristics and modelling heuristics.

Identification of requirements as well as their refinement is a preliminary step used towards achieving the set goals, as they are formulated at different levels of abstraction in respective documents.

As a result, the proposed taxonomy suggests aggregation of requirements with different granularity of functionalities in frameworks, from GAPP being the most granular and represented, to NIST as the most aggregated and set as fundamental (I1), with irrelevant concerns disregarded and 'overlaps' managed.

Subsequently, by characterizing the requirements and distributing them by respective attributes to the set taxonomy, qualitative values that can be used to ensure requirement pertinence to a specified goal representing a precise criterion for achieving the goal completeness are given.

Finally, derived entity-relationship metamodel can be used as a basis for further modelling heuristics in software and privacy policies engineering.

6.5.2 Limitations of research

Elaboration, as a significant part of GBRAM method, refers to analysing the set goals with consideration of possible obstacles and a detailed operationalization. Although the research lacks these heuristics to complete the goal-based requirement analysis, nevertheless, the proposed requirements accompanied with a detailed metamodel of their relationships of mutual association and/or dependence, can serve as a prerequisite for the development of transparency system functionalities through the use case scenarios. Further goal validation, alongside with taxonomy validation is in order.

6.6 Conclusion

Building effective transparency mechanisms in comprehensive environments of digital economy can be very challenging. It goes beyond efficient root factors of 'providing necessary information' and 'providing quality mechanisms', as effectiveness and efficiency are two separate terms. While efficiency is the state of achieving maximum productivity, with the least amount of effort expended, effectiveness is the extent to which something is successful in delivering the desired result. So, in the

long term, effectiveness is a strategic choice and transparency in the context of privacy engineering should be considered as such.

By modelling an effective TET metamodel based on heuristics-based approach abstracted statements about PI management were associated with the specific problem solutions or features that characterize a solution in the system application. Derived goals can be used as a cornerstone in the development of such systems: transparency goal—to stipulate general requirements in achieving transparency, the mechanism goal—that specifies requirements to realize quality of transparency mechanisms, the processing goal—that emerges from informing about personal information data flow, and the control goal—as a result of data subjects' rights to intervenability.

Subsequently, the resulting goals and applied methods can be used for a wider scope of research in directions that are related to scalability in terms of TET system quality as privacy management practices evolve to ensure more data security and risk management requirements in the prospects of new ePrivacy regulation.

References

[1] Sweeney L 2013 Discrimination in online ad delivery *Commun. ACM* **56** 44–54

[2] Datta A, Tschantz M C and Datta A 2015 Automated experiments on ad privacy settings *Proc. Priv. Enhancing Technol.* **2015** 92–112

[3] Calo R 2011 The boundaries of privacy harm *Indiana Law J.* **86** 1132–61

[4] Ranzini G, Etter M and Vermeulen I E 2017 Privacy in the sharing economy: european perspectives *SSRN Electron. J.*

[5] Bednar K, Spiekermann S and Langheinrich M *et al* 2019 Engineering privacy by design: are engineers ready to live up to the challenge? *Inf. Soc.* **35** 122–42

[6] do Prato, Leite J C S and Cappelli C 2010 Software transparency *Bus. Inf. Syst. Eng.* **2** 127–39

[7] Chung L, Nixon B A and Yu E 2000 *Non-Functional Requirements in Software Engineering* (Cham: Springer)

[8] Yu E S 1995 Modelling strategic relationships for process *PhD Thesis* University of Toronto

[9] do Orato, Leite J C S and Cappelli C 2008 Exploring i* characteristics that support software transparency *iStar'08, 3rd Int. i* Workshop* eds J Castro, X Franch, A Perini and E Yu https://ceur-ws.org/Vol-322/paper13.pdf

[10] Dabbish L, Stuart H C and Tsay J *et al* 2012 Social coding in GitHub: transparency and collaboration in an open software repository *Proc. ACM 2012 Conf Comput Support Coop Work* 1277–86

[11] Dabbish L, Stuart C and Tsay J *et al* 2013 Leveraging transparency *IEEE Softw.* **30** 37–43

[12] Serrano M and Do Prado Leite J C S 2011 Capturing transparency-related requirements patterns through argumentation *2011 1st Int. Work Requir. Patterns, RePa'11* 00 32–41

[13] Hosseini M, Shahri A and Phalp K *et al* 2015 Towards engineering transparency as a requirement in socio-technical systems *2015 IEEE 23rd Int. Requir. Eng. Conf. RE* 268–73

[14] Hosseini M, Shahri A and Phalp K *et al* 2016 Foundations for transparency requirements engineering *Lect. Notes Comput. Sci.* **9619** 225–31

[15] Hosseini M, Shahri A and Phalp K *et al* 2016 A modelling language for transparency requirements in business information systems *Lect. Notes Comput. Sci.* **9694** 239–54

[16] Hosseini M, Shahri A and Phalp K *et al* 2018 Four reference models for transparency requirements in information systems *Requir. Eng.* **23** 251–75
[17] Koehlinger J S 1990 Substantive due process analysis and the lockean liberal tradition: rethinking the modern privacy cases substantive due process analysis and the lockean liberal tradition: rethinking the modern privacy cases *Indiana Law J.* **65** 8
[18] Ponesse J 2014 The ties that bind: conceptualizing anonymity *J. Soc. Philos.* **45** 304–22
[19] Schermer B W 2011 The limits of privacy in automated profiling and data mining *C*omput. Law Secur. Rev. **27** 45–52
[20] Karegar F 2018 Towards Improving Transparency, Intervenability and Consent in HCI *Licentiate thesis* Karlstad University
[21] Zimmermann C 2015 A categorization of transparency-enhancing technologies arXiv:1507.04914
[22] Zimmermann C, Accorsi R and Müller G 2014 Privacy dashboards: reconciling data-driven business models and privacy *Int. Conf. on Availability, Reliability and Security*
[23] Dennedy M F, Fox J and Finneran T R 2014 *The Privacy Engineer's Manifesto* (Cham: Springer)
[24] OECD 2013 *The OECD Privacy Guidelines*
[25] Gellman R 2014 Fair information practices: a basic history *SSRN Electron J.*
[26] Asia Pacific Economic Cooperation 2015 APEC Privacy Framework
[27] National Institute of Standards and Technology 2020 NIST Privacy Framework - a tool for improving privacy through enterprise risk management
[28] Barrett M N 2018 Framework for improving critical infrastructure cybersecurity *Proc Annu ISA Anal Div Symp* **535** 9–25
[29] AICPA and Chartered Accountants of Canada 2009 Generally Accepted Privacy Principles
[30] Michener G and Bersch K 2013 Identifying transparency *Inf Polity* **18** 233–42
[31] Van Lamsweerde A 2001 Goal-oriented requirements engineering: a guided tour *Proc. IEEE Int. Conf. Requir. Eng.* 249–61
[32] European Commission 2016 General Data Protection Regulation
[33] Wright D and Raab C 2014 Privacy principles, risks and harms *Int. Rev. Law, Comput. Technol.* **28** 277–98
[34] Cate F H 2006 The failure of fair information practice principles *Consumer Protection in the Age of the Information Economy* (Aldershot: Ashgate Publishing)
[35] Anton A I and Potts C 1998 Use of goals to surface requirements for evolving systems *Proc. Int. Conf. on Software Engineering* 157–66