Towards Legal Privacy Risk Assessment and Specification

Ebenezer Paintsil

Department of Applied Research in ICT
Norwegian Computing Center
Oslo, Norway
paintsil@nr.no

Abstract. This article focuses on privacy risk assessment from a legal perspective. We focus on how to estimate legal privacy risk with legal norms instead of quantitative values. We explain the role of normative values in legal risk assessment and introduce a specification for legal privacy risk using a modal language. We examine the difference between legal privacy risk assessment and Information Technology (IT) security risk assessment. IT security risk assessment supports the decision-making processes of system stakeholders - individuals, managers, groups or organizations. It supports both quantitative and qualitative risk analyses and may rely on the knowledge of security experts to estimate the risk. The application of an IT security risk assessment method for legal privacy risk assessment may lead to poor communication and high uncertainties in the risk estimation because legal reasoning is based on normative values and requires legal knowledge. This article proposes legal privacy risk assessment in the knowledge domain of a legal risk assessor.

1 Introduction

An Information Technology (IT) risk assessor can facilitate communication and reduce uncertainty in IT risk assessment if the assessment is done in the risk assessor's knowledge domain [1]. Traditional IT security risk assessment may employ quantitative, qualitative or semi-quantitative values to estimate or report risk [1], [2]. The risk estimation techniques may reflect the goal of an organization [3], [4] or the experience of the security risk assessor since IT risk assessment depends on the risk assessors' experience [1]. For example, the Risk IT [4] management framework relies on the COBIT Information Criteria, Balanced Scorecard Criteria, COSO and Westerman techniques to communicate risk impact to system owner - the organization. These communication techniques are organization-focused because they express risk impact in business and financial terms. They intend to communicate risk to the policy makers or the system owners but not to others system stakeholders.

Similarly, the AS/NZS:4360 [5] risk management standard (now ISO 31000), the NIST [6], OCTAVE [7], CORAS [8] and ISO27005 [9] are mainly security-focused, assets driven, organization-oriented [3] and use qualitative, quantitative or semi-quantitative values to estimate risk (see [1], [2]).

S. Furnell, C. Lambrinoudakis, and G. Pernul (Eds.): TrustBus 2011, LNCS 6863, pp. 174–185, 2011.

However, privacy has security as well as legal perspective. We may effectively communicate and estimate the legal privacy risk with normative values rather than quantitative values. This is because quantitative values may not make legal sense in legal risk assessment since legal decision-making is based on normative values rather than quantitative values. Moreover, they may not effectively communicate risk or uncertainty to a lawyer who may assess the legal aspect of the privacy risk.

The objective of this article is to explain the importance of legal norms in privacy risk assessment and to examine the difference between legal privacy risk assessment and IT security risk assessment. Further, we introduce a conceptual model for legal privacy risk assessment leading to an attempt towards logical formalizations of legal privacy risk.

The rest of the article is organized as follows. In Section 2, we introduce existing works on privacy risk assessment. We examine other approaches to privacy risk assessment and protection. Section 3 is the overview of the legal risk assessments' concepts focusing on how the legal aspect of privacy contributes to privacy risk assessments. We introduce a conceptual model for legal privacy risk assessment in section 4 and the language for the legal risk specification in section 5. Section 6 is the legal privacy risk specification. Finally, section 7 states the conclusion and future work.

2 Related Work

The Platform for Privacy Preferences (P3P) is a protocol for expressing privacy policy in both a machine and human readable way using a standard XML schema [10]. The standard schema allows the service provider to use a set of predefined terms to describe their privacy policy. The privacy policy may specify the kind of data the web site collects, dispute resolution procedure, how long data will be retained and how the personal data will be used. Furthermore, the World Wide Web Consortium (W3C) designed a Platform for Privacy Preferences Preference Exchange Language (APPEL) to enable individuals to express their privacy preferences, to query the data represented by P3P, and to make decisions accordingly [10]. However, P3P and APPEL focus on privacy policies, but not legal reasoning.

Furhermore, Ardagna et al. introduced the PrimeLife policy language for privacy enforcement [11]. The language uses modalities such as temporal constraints, pre-obligations, conditional obligations, and repeating obligations to model different types of obligations. It uses authorization modality to specify data transfer competence. Rules have two modalities, permit or deny. The language uses the concept of trusted credentials and specifies the agreement between a data controller and a data subject as a promise. The language focuses on empirical specification instead of legal specification. The obligation and authorization modalities used in the language are not expressive enough to embrace all aspect of legal reasoning. Legal reasoning has several modalities including right, permission, obligations, exceptions, rule, power and commitment.

Berthold [12] introduces the language for privacy options which is an adaptation of the financial contracts language proposed by Peyton Jones and Eber [13]. Similarly, Mahler introduces a legal risk assessment approach focusing on legal contract and communication [14]. Yet, legal privacy risk is not necessarily contractual; it depends on the nature of the applicable law. A regulatory framework permits both norm of conduct (command or permission) and competence (power) [15], [16]; however, mandatory law may permit no competence norm. Hence, it is not clear that a contractual risk model is appropriate for legal privacy risk assessment. Another limitation of the contractual approach to privacy risk modeling is that the approach focuses on those who explicitly declare their consent or enter into a contractual agreement with a data controller regarding the protection of their personal data. This means, where there is no contractual agreement, such model may fail to apply.

Wang introduces five requirements for security metrics including the requirement for quantitative metric [2]. Quantitative metrics reduce subjectivity and increase the level of trust. However, Aven disagrees with these assertions. He argues that the arbitrariness in quantitative risk estimation “”could be significant, due to the uncertainties in the estimates or as a result of the uncertainty assessment being strongly dependent on the assessors” [1]. He introduced a mixed approach called the semi-quantitative approach which combines both quantitative and qualitative estimation techniques in order to assess the risk. The approach is intended to reduce the uncertainties in quantitative risk analysis (QRA). Nevertheless, Aven did not consider the effect of semi-quantitative approach on legal risk communication and reasoning since legal risk depends on normative values instead of semi-quantitative values.

CORAS [17] uses the unified modeling language (UML) to model a targeted system. It then employs complementary risk management methods to assess different models of the targeted system. CORAS risk management method facilitates communication and interaction among stakeholders. However, CORAS is asset or security-oriented, focusing on asset protection and estimates legal risk based on quantitative values [8, p.327-337] instead of normative values.

3 Legal Risk Assessments and Privacy

Legal propositions or norms and “”normative values” are central to legal risk assessment. We regard normative values as standards for assessing legal reasoning. They include obligation, permission, exception and right. We refer to them as legal modalities. Normative values may be referred to as norms [15], [16]. A legal norm consists of facts (legal antecedents or something that must happen before) and consequences [18]. The antecedent describes which factual circumstances have to be present for a normative value to apply. The consequent indicates the legal implications of the applicable normative value. Thus, normative values may connect a legal antecedent to a legal consequent or determine the transition from legal antecedent to legal consequent.

Legal antecedent is either a fact or a proposition. A fact is something that is established to be true and may not be disputed. A proposition is something that is true, believed to be true, known to be true, ought to be true, eventually true or is necessarily true. We refer to the words "ought to, believe, known, eventually and necessary" as the modalities of the proposition.

We refer to legal modalities as normative values and categorize them as normative values for conduct, competence and right. The normative values for conduct (command) require a stakeholder to conditionally perform an action [19]. The competence normative values confer public or private power, immunity, subjection, disability etc. on a legal person [15], [16]. They may determine the validity of legal power or capacity. Legal competence may grant the capacity to create legal rules binding others or oneself. Legal right permits a stakeholder to conditionally perform an action that may advance his/her interest or the interest of others.

The normative values are obligation, permission, prohibition, commitment, rule, authority, power, right, responsibility, and exception [20], [16]. "Facultative" is a special kind of normative value which permits an action and its negation [16]. Unlike traditional risk assessment, normative values may play an important role in legal risk assessment. Nevertheless, their thorough analysis and relationships are beyond the scope of this article. However we provide the Black Dictionary definitions as follows[1]:

- **Obligation:** a legal or moral duty to do or not to do something
- **Permission:** a license or liberty to do something
- **Prohibition:** a law or order that forbids a certain action
- **Commitment:** an agreement to do something in future
- **Rule:** to command or require to do something
- **Authority:** the right or permission to act legally on someone's behalf
- **Power:** the ability to act or not act
- **Right:** a power, privilege or immunity secured to a person by law
- **Responsibility:** liability or the quality, or state of being legally obligated or accountable
- **Faculty:** an authorization granted to someone to do what otherwise would not be allowed

How we choose an applicable legal norm depends on the applicable law. The mandatory or regulatory character of the rules laid down in the applicable privacy law determines the applicable legal norm. Rules of mandatory law are generally rules from which the parties cannot derogate by contract [23],[24]. Generally, the right to withdraw from a contract and protection against unfair contractual terms are mandatory rules.

Similarly, the applicable normative values for privacy risk depend on the nature of the privacy law or regulation. Deciding the nature of an applicable privacy law is not a straightforward matter. For instance, it is not clear that the nature

[1] For more information on norms refers to [21],[22], [15], [16].

of rules laid down in the European Union (EU) data protection directive (DPD) [25] is rules of mandatory law.

Cuijper [24] argues that the EU DPD does not require implementation into mandatory rules of law. The objectives focus on individual protection with regard to processing of personal data and free movement of personal data. She emphasized the latter as more important. The regulation for free movement of personal data does not mandate the implementation of the DPD into mandatory rules of law. In addition, Cuijper stressed that the directive contains no clause requiring mandatory law and DPD article 7 [25] leaves room for processing of personal data based on contract. She concluded that, “”it will be a step too far to denounce judicial effect to all contracts between data controllers and data subjects in which the data subject willingly gives up part of the rights granted to him on the basis of this directive”.

However, Bergkamp argues otherwise. According to Bergkamp the “”DPD establishes a public law regime that cannot be varied by a private law contract” [26, p. 123]. Even Cuijper [24] noted that, the argument for private law regime depends on whether the data subject has a strong bargaining power. In cases where the data subject is the weaker party, the law may have to give the subject a strong protection. In addition, the data controller may process personal data under the EU DPD without a contractual agreement [27]. The lack of legal consensus between the public and private law character of the DPD represents legal uncertainty that can contribute to legal privacy risk. Furthermore, the nature of the applicable privacy law is an important modality to consider in legal privacy risk assessment because it determines the applicable normative values.

4 Legal Privacy Risk Assessments Conceptualization

Currently, there are over 200 risk management methods with no adequate selection criteria [28]. We selected the CORAS [8] because it is a well-documented risk assessment method, has straightforward risk assessment concepts and attempts to model legal risk. CORAS manages risk in eight steps but the central concepts revolve around the combined effect of threat, vulnerability, threat scenario, unwanted incident on an asset [8]. A threat exploits vulnerabilities in an asset, leading to a chain of events called threat scenario that may lead to unwanted incident that may in turn cause loss to a system owner or a stakeholder.

Figure 1 depicts a risk assessment conceptual model based on the CORAS risk assessment concepts. It also depicts one of the fundamental differences between legal risk assessment and information technology (IT) security risk assessment. Figure 1(a) represents a simple IT security risk assessment scenario and 1(b) is the legal risk assessment scenario. Quantitative values determine the transitions in Figure 1(a) reflecting a good security risk assessment [2]. Nevertheless, the transitions in Figure 1(b) are determined by normative values (obligations) reflecting legal decision-making. Legal decision-making depends on normative values rather than quantitative values and transition decisions depend on the legal rule(s).

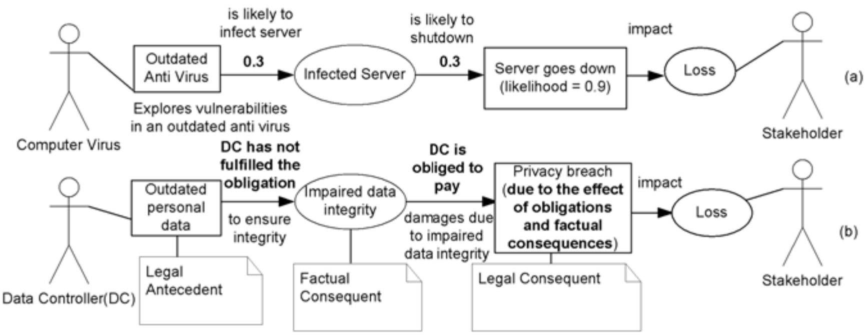

Fig. 1. Diagram (a) Represents a Simple Security Risk Assessment Scenario and (b) is a Simple Legal Privacy Risk Assessment Scenario

Unlike IT security risk assessment, legal risk assessment relies on legal antecedents, normative values and legal consequents to determine the effect of a legal breach [18], [14]. Therefore a risk assessment method based on quantitative values may not make legal sense. We determine the risk by measuring the extent by which the legal breach impact on the objectives of a stakeholder. This is referred to as risk tolerance [4]. We have privacy risk if the loss is higher than the acceptable risk level or risk tolerance. The risk tolerance and the decision to arrive at the loss should be deduced from the legal rules and applicable case laws.

In Figure 1(b) a legal antecedent may lead to a factual consequence. Legal antecedents may consist of one or more facts that may lead to a factual consequent. They have both legal propositions and factual propositions. This conceptualization highlights one of the possible ways of reasoning about legal privacy risk. The directed graph and the normative values could make it possible to use hybrid modal logics for the legal privacy risk specification leading to a possible automation. Consequently, we model legal privacy risk as a directed graph with normative values that determine the transitions leading to a loss.

5 The Privacy Risk Specification Language

We introduce a language for privacy risk specification language. The language is based on deontic, hybrid modal and propositional dynamic logics. Modal logics are highly expressive and suitable for directed graph (see [29]). They provide a good balance between expressiveness and complexity. Most importantly modal logics are syntactically simple language and mathematically rich [30, p. xii-x].

We model the privacy risk as a directed graph. A directed graph or a relational structure is a set of nodes and edges between them [29]. It is defined as $\langle W, R \rangle$ where W is non-empty set of vertices of the relational structure called the worlds or a states. The members of W represent the states, points, nodes, instants or situations of the relational structure. The R is the set of edges of the relational structure representing the accessibility relation between worlds. The cross product $\{W \times W\}$ stands for $\{(w_1, w_2)|w_1 \in W, w_2 \in W\}$ is the set of all ordered pairs (w_1, w_2) where w_1 and w_2 are members of W. The set $R \subseteq W \times W$ is the binary or accessibility relation over W. A model in modal logic is a relational structure with valuation i.e. $M = (W, R, V)$ where V is the valuation. The valuation determines the truth or falsity of a proposition or a formula.

Hybrid modal logic extends the traditional modal logic. In addition to the set of proposition at each world, hybrid modal logic introduces special propositional symbol known as nominal. A nominal is true at exactly one world of a model [31]. Hence, we can use it to name a state. Further, hybrid modal logic introduces a state variable. A state variable is an atomic formula denoting a state. Hybrid logic has additional operators: @ and $\downarrow$. The $\downarrow$ is known as the binder. It is possible to express irreflexivity of a state with the binder. Using $\downarrow$ allows one to name a world where a formula $\downarrow x\Psi$ will be evaluated. The x is a state variable or a nominal and Ψ is a formula. $\downarrow x\Psi$ binds all the occurrences of x in Ψ to the current state where the evaluation is occurring [31]. The @ operator allows a "jump" from the current world to another world or a state in a frame. For example, the formula $@_x\Psi$ is true if Ψ is true at the world denoted by x.

Modal logics express modalities. The basic modalities are necessarily and possibly. The necessarily modality is represented by a box $[]$. Also, the possibly modality is represented by a diamond $\langle\rangle$. The symbols for the modalities can be empty or non-empty. The empty box $[]$(necessarily or obligation) means the evaluation statement is true in every one-step successor of the current world of the model. Similarly, empty diamond $\langle\rangle$ symbol modality (possibly modality or permission) means the evaluation of the modal formula is possible in some one-step successor of the current world of the model [31], [32], [33].

Propositional dynamic logic is another kind of modal logics. It may be used to express action. The actions are included in the necessary or the possibly box. The non-empty necessarily box $[\pi]\beta$ in propositional dynamic logic means every execution of π from the current state leads to the states bearing the information β [30, p. 13]. Similarly, the non-empty possibly modality $\langle\pi\rangle\,\beta$ means some terminating execution of π from the current state leads to the states bearing the information β. Also, we can refer to β as a formula or a proposition that hold in a necessary or possible world or the consequence of an action (proposition or legal rules) π.

We note that the following complex relations hold:

- If π_1 and π_2 are programs, then so is $\pi_1 \cup \pi_2$ – executes π_1 or π_2
- If π_1 and π_2 are programs, then so is $\pi_1; \pi_2$ – executes π_1 and then π_2
- If π is a program then so is π^* – executes π zero or finite number of times
- If π_1 and π_2 are programs, then so is $\pi_1 \cap \pi_2$ – executes π_1 and π_2 in parallel
- If β is a formula, then $\beta?$ is a program that test whether β holds, if so the execution continues; else it stops

We use Deontic logic [20], [16] to express the legal rules that may determine the effect of an action or a fact and dynamic proposition logic for the actions or factual propositions. We can express a proposition in a form of an action and vice versa. Deontic logic is used to express legal obligations. In order to express the legal modalities in deontic logic, we group the normative values into three groups (legal competence, conduct and legal right) and introduce the notation ${}^{P}L^{A}_{(C,D,R)}$ to express the legal rules or propositions. The modality C represents a set of competence norms; D is a set of conduct norms, and R is a set of right norms. The notation ${}^{P}L^{A}_{(r)}(\beta)$ represents legal right, meaning the stakeholder P may perform the action β in order to advance the interest of A, where $r \in R$. P is the same as A when one performs an action to advance his/her own interest.

The following are the syntax and semantic of the specification language.

- Let the basic unanalyzed proposition or atomic formula $prop := p, q, r ... and\ \top\ ''always\ true'', \bot\ ''always\ false''.$
- Let the set of nominal $NOM = \{n1, n2, n3...\}$.
- Let the set of state variables $SV = \{s1, s2, s3...\}$.
- The binary connective $\wedge$.
- The unary connective $\neg$.
- Let the finite set of programs or propositions $PI = \{\pi_1, \pi_2, \pi_3 ... \pi_n\}$.
- The unary operator $[\pi]$ where $\pi \in PI$.
- The unary operator $\langle\pi\rangle$ where $\pi \in PI$.
- The binder operator $\downarrow$
- The $@_x$ where x is a state variable or nominal.

$\theta := prop|\neg\varphi|(\varphi \wedge \phi)|(\varphi \vee \phi)|(\varphi \rightarrow \phi)|[\pi]\varphi|\langle\pi\rangle\varphi|[]\varphi|{}^{P}L^{A}_{(C,D,R)}(\pi)$ where $\pi \in PI$
We write a formula that is true at a world w of a model $M = (W, R, V)$ as $M, w \models \varphi$. It follows that

- $M, w \models p$ iff $w \in V(p)$ where $p \in prop$
- $M, w \models \neg\varphi$ iff not $M, w \models \varphi$
- $M, w \models \varphi \wedge \phi$ iff $M, w \models \varphi$ and $M, w \models \phi$
- $M, w \models @_x\varphi$ iff $M, x \models \varphi$ where $x \in SV$
- $M, w \models \varphi \rightarrow \phi$ iff not $M, w \models \varphi$ or $M, w \models \phi$

We refer to this as Kripke semantics, named after Saul Kripke [29].

6 Legal Privacy Risk Specification

We consider an example of the application of the language in this section. We consider the DPD article 6 (data quality) and article 23 [25] with reference to Figure 2. We manually extract the normative values following the example in [19]. The result of the simplified extraction is shown in Table 1.

The normative phrase determines the normative values. The extraction program will extract the normative values depending on the normative phrase. For example the normative phrase “”Must” implies obligation and “”May or Can” implies right (see [19]). We specify the legal privacy risk with the language described in section 5 with reference to the model in Figure 2.

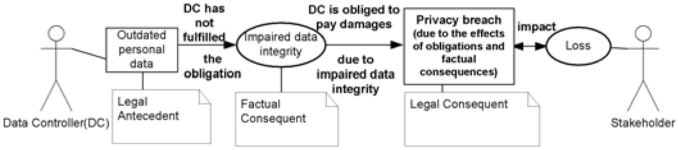
DC has not fulfilled the obligation
DC is obliged to pay damages due to impaired data integrity
Outdated personal data
Impaired data integrity
Privacy breach (due to the effects of obligations and factual consequences)
impact
Loss
Legal Antecedent
Factual Consequent
Legal Consequent
Data Controller(DC)
Stakeholder

Fig. 2. A Simple Legal Privacy Risk Assessment Scenario

Table 1. Extracted Legal Normative Values

Rule No.	Norm Proposition (Rule)	Normative Phrase	Normative Value
R1	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes	must	obligation
R2	Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards	Shall not	not obligation
R3	Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed	must	obligation
R4	DPD aricle 23: Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act to this Directive incompatible with the national provisions adopted pursuant is entitled to receive compensation from the controller for the damage suffered	shall	obligation

In modal logics, a world has a set of propositions and is accessible from another world. We assume that each of the entities Legal Antecedent, Factual Consequent, Legal Consequent and Loss in Figure 2 are accessible from other worlds. Therefore, they are the possible worlds or states which we represent by w_{la}, w_{fc}, w_{lc} and w_l respectively. The set of the possible worlds or the universe is $W = \{w_{la}, w_{fc}, w_{lc}, w_l\}$. The analysis of a scenario or a legal proposition may lead to a program execution that may in turn lead to a new state or world. We assume that it is possible to access the Loss state from the Legal Consequent state in both directions as in Figure 2. We represent each state w_{la}, w_{fc}, w_{lc} and w_l with a set of nominal, $\{la, fc, lc, l\}$ respectively. Each state has a set of legal and factual propositions. Let C, D, R represent the set of competence, conduct and legal right norms respectively. Table 2 presents the analysis of factual prepositions and legal rules.

Table 2. Legal Privacy Risk Assessment

ID	Legal Assessment	Normative Value	Formula
L1	is outdated data leads to impaired data integrity (According to DPD article 6(e) (R4 in Table 1) personal data must be accurate and, where necessary, kept up to date)	Obligation	${}^P L^A_{(o)}(\pi_1)$ π_1 is "accurate and up to date data" $o \in D$ where D is the set of conduct norms
L2	is impaired data integrity is illegal (According to DPD article 23 (R4 in Table 1) violations shall lead to damages)	Obligation	${}^P L^A_{(o)}(\pi_2)$ π_2 is “”stakeholder entitled to receive compensation from the controller for the damage suffered” $o \in D$ where D is the set of conduct norms

$$PossibleRisk := @^P_{la} L^A_{(o_1)}(\pi_1) \wedge \langle \pi_1(F_1)? \rangle \wedge^P L^A_{(o_2)}(\pi_2) \wedge \langle \pi_2(F_2)? \rangle$$
$$\downarrow_x ({}^P L^A_{(C,D,R)}(\pi_3) \wedge \langle \pi_3(F_3)? \rangle\, \alpha \wedge \langle tolerate(\alpha)? \rangle_x) \ldots (1)$$

Where F_1, F_2, F_3 are the facts, π_1, π_2 and π_3 are functions, $o_1, o_2 \in D$, α is the consequences of the legal rules and facts, $tolerate(\alpha)$ is a test program for risk tolerance.

Equation (1) is a legal privacy risk specification. We begin the legal privacy risk assessment at the state w_{la} (the Legal Antecedent state). The formula $@^{P}_{la}L^{A}_{(o_1)}(\pi_1) \wedge \langle \pi_1(F_1)? \rangle$ evaluates at the Legal Antecedent's state. The formula ${}^{P}L^{A}_{(o_1)}(\pi_1)$ expresses the legal proposition for the available fact. The formula $\langle \pi_1(F_1)? \rangle$ checks if the fact F_1 violates the legal rule (π_1) and makes a transition to the factual consequent's state otherwise the execution is stopped. We repeat a similar process at the Factual Consequent state. The formula $({}^{P}L^{A}_{(C,D,R)}(\pi_3) \wedge \langle \pi_3(F_3)? \rangle\, \alpha)$ estimates the consequence α based on the appropriate privacy legal rules. The formula $\downarrow_x\ ({}^{P}L^{A}_{(C,D,R)}(\pi_3) \wedge \langle \pi_3(F_3)? \rangle\, \alpha \wedge \langle tolerate(\alpha)? \rangle_x)$ is a test program. It returns to the current state or the Legal Consequent's state(w_{lc}) if the stakeholder can tolerate the loss. The transition $\langle \pi_3(F_3)? \rangle$ leads to the Loss state. The Loss state then evaluates the impact for the possible loss and return to the Legal Consequent state if the stakeholder can tolerate the loss.

The possible legal privacy risk is the transition from the Legal Antecedent's state to the Loss state. We represent the transition by the formua (1) or *PossibleRisk*. The formula *PossibleRisk* is satisfied if the stakeholder can tolerate the legal privacy risk, otherwise the estimated loss is inconsistent with the objectives of the stakeholder and therefore we may transfer, avoid, mitigate or share the risk. We can generalize the *PossibleRisk* formula by understanding the effects of possible combinations of legal norms and facts. The formula *PossibleRisk* is an example of a simple logical specification of legal privacy risk.

7 Conclusion

Legal privacy risk depends on the applicable normative values determined by the nature of rules of the legal provision (regulatory or mandatory rules of law). It is not concerned with the protection of physical assets and estimation of quantitative values but considers the effect of normative values on facts or legal antecedents. In this article, we focus on making legal privacy risk assessment more meaningful to information technology (IT) professional by introducing a legal privacy risk assessment conceptual model. Further, we propose a language based on hybrid modal logic, propositional dynamic logic and deontic logic as a possible tool for legal privacy risk specification. We exemplify legal privacy risk specification with the language. Although the specification is simple and case specific, it highlights one of the possible ways of assessing legal privacy risk and how legal privacy risk assessment differs from IT security risk assessment. We can build on this initial insight to automate legal privacy risk assessment. Our future work will investigate how to improve the specification by relaxing some of the assumptions. We will focus on the complexities of combining facts and legal norms in legal privacy risk estimation and the effect of legal uncertainty on legal privacy risk estimation. We will provide a general specification for legal privacy risk automation.

Acknowledgment. The work reported in this paper is part of the PETweb II project sponsored by the Research Council of Norway under grant 193030/S10.

References

[1] Aven, T.: A semi-quantitative approach to risk analysis, as an alternative to qras. Reliability Engineering & System Safety 93(6), 790–797 (2008)

[2] Wang, A.J.A.: Information security models and metrics. In: ACM-SE 43: Proceedings of the 43rd Annual Southeast Regional Conference, pp. 178–184. ACM, New York (2005)

[3] Strecker, S., Heise, D., Frank, U.: Riskm: A multi-perspective modeling method for it risk assessment. Information Systems Frontiers (2010)

[4] ISACA: The Risk IT Practitioner Guide. ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA (2009) isbn: 978-1-60420-116-1

[5] Committee, A.Z.S.: Risk management as/nzs4360:1999. Technical report, Standards Australia (1999)

[6] Gary, S., Goguen Alice, F.A.: Nist special publication 800-30 risk management guide for information technology systems. Technical report, National Institute of Standards and Technology (2002)

[7] Christopher, A., Dorofee Audrey, S.J.W.C.: Introduction to the octave approach, vol. 37. Carnegie Mellon Software Engineering Institute (2003)

[8] Lund, M.S.: Bjørnar Solhaug, K.S.: Model-Driven Risk Analysis, The CORAS Approach, 1 edn. Springer, Heidelberg (2011) 978-3-642-12322-1

[9] ISO: Iso 27005 information security risk management. Technical report, International Organization for Standardization (2008)

[10] Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J.: The platform for privacy preferences 1.0 (p3p1.0) specification (2002), http://www.w3.org/TR/P3P/

[11] Ardagna, C., Bussard, L., De Capitani di Vimercati, S., Neven, G., Paraboschi, S., Pedrini: PrimeLife Policy Language. In: W3C Workshop on Access Control Application Scenarios, Luxembourg (2009)

[12] Berthold, S.: Towards a formal language for privacy options. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.) Privacy and Identity 2010. IFIP Advances in Information and Communication Technology, vol. 352, pp. 27–40. Springer, Heidelberg (2011) 10.1007/978-3-642-20769-3_3

[13] Jones, S.E.P.: How to write a financial contract. Macmillan Publishers Limited, Palgrave Macmillan, Oxford (2003)

[14] Mahler, T.: Legal Risk Management Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts. Monograph, The Faculty of Law, University of Oslo, Postboks 6706 St Olavs Plass, 0130 Oslo Norway (2010)

[15] Bulygin, E.: On norms of competence. Law and Philosophy 11(3) (1992)

[16] Sartor, G.: Fundamental legal concepts: A formal and teleological characterisation. Artificial Intelligence and Law 14, 101–142 (2006)

[17] Stølen, K., Braber, F.D., Dimitrakos, T., Fredriksen, R., Gran, A., hilde Houmb, S., Lund, M.S., Stamatiou, Y.C., Aagedal, J.Ø.: Model-based risk assessment the coras approach. In: Presented at the 1st Itrust Workshop (2002)

[18] Vraalsen, F., Lund, M.S., Mahler, T., Parent, X., Stølen, K.: Specifying legal risk scenarios using the CORAS threat modelling language. In: Herrmann, P., Issarny, V., Shiu, S.C.K. (eds.) iTrust 2005. LNCS, vol. 3477, pp. 45–60. Springer, Heidelberg (2005) 10.1007/11429760_4

[19] Kiyavitskaya, N., Zeni, N., Breaux, T.D., Antón, A.I., Cordy, J.R., Mich, L., Mylopoulos, J.: Extracting rights and obligations from regulations: toward a tool-supported process. In: Proceedings of the Twenty-Second IEEE/ACM International Conference on Automated Software Engineering, ASE 2007, pp. 429–432. ACM, New York (2007)

[20] Encyclopedie, D.L.I.: Deontic logic. IVR Encyclopedie (2010)

[21] Jones, A.J.I., Sergot, M.J.: A formal characterisation of institutionalised power. Logic Journal of the IGPL 4(3), 427–443 (1996)

[22] Hart, H.: The Concept of Law, 2nd edn. Clarendon Press, Oxford (1994) isbn:0-19-876123-6.

[23] Edwards, L.: The New Legal Framework for E-Commerce in Europe. Hart Publishing, Oxford (2005) ISBN 13:978-1-84113-451-2

[24] Cuijpers, C.: A private law approach to privacy; mandatory law. SCRIPTed 4:4(318) (2007)

[25] Commission, E.: 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. Technical report, European Parliament (1995)

[26] Bergkamp, L.: European Community Law for the New Economy. Intersentia Publishers, Antwerp, Oxford, New York (2003) ISBN:90-5095-229-1

[27] Olsen, T., Mahler, T.: Identity management and data protection law: Risk, responsibility and compliance in 'circles of trust'. Computer Law & Security Report 23(4), 342–351 (2007)

[28] Matulevičius, R., Mayer, N., Mouratidis, H., Heymans, P., Genon, N.: Adapting secure tropos for security risk management in the early phases of information systems development. In: Bellahsène, Z., Léonard, M. (eds.) CAiSE 2008. LNCS, vol. 5074, pp. 541–555. Springer, Heidelberg (2008)

[29] Blackburn, P., van Benthem, J.: Modal logic: A semantic perspective. ETHICS 98, 501–517 (1988)

[30] Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic. Cambridge University Press, Cambridge (2010) isbn:978-0-521-80200-0

[31] Bidoit, N., Cerrito, S., Thion, V.: A first step towards modeling semistructured data in hybrid multimodal logic. Journal of Applied Non-Classical Logics 14(4), 447–475 (2004)

[32] Areces, C., ten Cate, B.: Hybrid logics. In: Blackburn, P., Wolter, F., van Benthem, J. (eds.) Handbook of Modal Logics. Elsevier, Amsterdam (2006)

[33] Blackburn, P., Ten Cate, B.: Pure Extensions, Proof Rules, and Hybrid Axiomatics. Studia Logica 84, 277–322 (2006)